LAPIN AMK
Lapland University of Applied Sciences

Tornion kuumavalssaamon IT-palveluiden kehityssuunnitelma

Hannu Tauriainen

Teollisuuden ja luonnonvarojen osaamisalan opinnäytetyö
Teknologiaosaamisen johtamisen
Insinööri (Ylempi AMK)

KEMI 2014

ALKUSANAT

Tämä opinnäytetyö on tehty Outokumpu Oyj:n toimeksiannosta. Opinnäytetyö on tehty syksyn 2013 ja kevään 2014 aikana.

Haluan kiittää opinnäytetyön ohjaajia Jaakko Ettoa ja Tuomo Aroa hyvistä neuvoista ja sujuvasta työn ohjauksesta. Kiitokset kuuluvat myös työkavereilleni hyvästä yhteistyöstä.

Suurimmat kiitokseni haluan esittää perheelleni ja ennen kaikkea vaimolleni kannustuksesta ja opintojeni tukemisesta.

Kemissä 6.5.2014

Hannu Tauriainen

TIIVISTELMÄ

LAPIN AMMATTIKORKEAKOULU, Teollisuuden ja luonnonvarojen osaamisala

Koulutusohjelma:	Teknologiaosaamisen johtaminen
Opinnäytetyön tekijät:	Hannu Tauriainen
Opinnäytetyön nimi:	Tornion kuumavalssaamon IT-palveluiden kehityssuunnitelma
Sivuja (joista liitesivuja):	54 (14)
Päiväys:	6.5.2014
Opinnäytetyön ohjaajat:	DI Jaakko Etto DI Tuomo Aro

Tämä opinnäytetyö on tehty Outokumpu Oyj:n IT-organisaatiolle. Opinnäytetyön tavoitteena oli kartoittaa Tornion kuumavalssaamon IT-palveluun kuuluvien ja vielä kuulumattomien järjestelmien nykytilanne ja tehdä riskianalyysi niiden pohjalta. Riskianalyysin tavoitteena oli tunnistaa kriittisimmät tehdasjärjestelmät, tehdä suunnitelmat havaittujen riskien ehkäisemiseksi sekä luoda IT-palveluista kehityssuunnitelma seuraavaksi neljälle vuodelle

Opinnäytetyön teoriaosa koostuu tietojärjestelmien riskienhallinnasta. Käytetyn teorian mukaan jokainen IT-järjestelmä on jollain tavoin haavoittuvainen ja siksi riskienhallinnan on oltava jatkuvatoiminen prosessi. IT-järjestelmien merkitys liiketoiminnalle on kasvanut merkittävästi viime vuosina ja yhä useampi liiketoiminta on riippuvainen IT-järjestelmistä.

Opinnäytetyö on toteutettu kvalitatiivisena tutkimusmenetelmänä, jossa on hyödynnetty toimintatutkimuksen tuomaa näkökulmaa. Työn tarkoituksena on ollut löytää konkreettisia parannusehdotuksia, eli miten tehdasjärjestelmät saataisiin tulevaisuudessakin pysymään vähintään yhtä toimintavarmoina ja tukemaan liiketoimintaan ja sen antamia vaatimuksia.

Opinnäytetyön tuloksena syntyi laaja käsitys kuumavalssaamon tehdasjärjestelmien toiminnoista, nykytilasta ja niiden merkityksestä liiketoiminnalle. Suurin osa kuumavalssaamon tehdasjärjestelmien riskeistä on hyvässä hallinnassa, mutta työ tulee vaatimaan jatkuvaa panostusta ja osassa järjestelmissä jopa välittömiä toimenpiteitä.

Asiasanat: Riskienhallinta, riskianalyysi, prosessinohjaus, tuotannonohjaus, kehityssuunnitelma

ABSTRACT

LAPLAND UNIVERSITY OF APPLIED SCIENCES,

Technology

Degree programme:	Technology Competence Management
Authors:	Hannu Tauriainen
Thesis title:	Development plan for IT Services at Tornio Hot Rolling Mill
Pages (of which appendixes):	54 (14)
Date:	6th May 2014
Thesis instructors:	MSc (el. eng) Jaakko Etto, MSc (el. eng) Tuomo Aro

This thesis had been made for IT organization of Outokumpu Oyj. The objective of the thesis was to survey the current state of the production systems at Tornio Hot Rolling Mill, and create a risk analysis for them. The survey was set to cover both the systems which were included in the IT-service network, as well as the systems that were not. The target of the risk analysis was to recognize the most critical production systems, create plans for preventing the detected risks and create a development plan for IT-services for the next four years.

The theoretical part of the thesis consists of risk management in information technology. According to used theory, every IT system is vulnerable and therefore the risk management has to be a continuous process. In recent years, the relevance of the IT systems to business has increased and nowadays business is more depending on IT systems.

This thesis had been implemented as a qualitative research and the point of view from action research has been employed. The purpose of the work is to find concrete suggestions for improvements. In other words, how IT systems could at least sustain their current level of reliability and keep supporting the requirements of the business also in the future.

The result of the thesis was a comprehensive understanding for the functionalities and the current state of the production systems and their relevance to the business. Most risks in the production systems of hot rolling mill are in good control but risk management will keep require continuous work, while some specific systems require immediate actions.

Keywords: risk management, risk analysis, process control, production control, development plan.

SISÄLLYS

KÄYTETYT MERKIT JA LYHENTEET

Alpha	Askelpalkkiuunien prosessinohjausjärjestelmä
APU	Askelpalkkiuuni
COS	Kupu-uunien prosessinohjausjärjestelmä
HotSIS	Kuumavalssaamon pinnantarkistusjärjestelmä
ICT	Information and Communication Technology, suom. tieto- ja viestintätekniikka
IT	Information Technology, suom. informaatioteknologia, tietotekniikka
JTSU	Jaloterässulatto
KUVA	Kuumavalssaamo
L0	Kenttälaitetaso (ISA-95 standardi)
L1	Automaatiotaso (ISA-95 standardi)
L2	Prosessinohjaustaso (ISA-95 standardi)
L3	Tuotannonohjaustaso (ISA-95 standardi)
L4	Toiminnanohjaustaso (ISA-95 standardi)
MTS	Myynnin ja tuotannonsuunnittelun tietojärjestelmä
PIHA	Pinnanlaadun hallinta-järjestelmä kylmävalssaamolla
PMS	Plant monitoring system, valssauslinjan kunnonvalvontajärjestelmä
QMato	Terässulaton ja kuumavalssaamon tuotannonohjausjärjestelmä
SMSD	Valssauslinjan prosessinohjausjärjestelmä
VASE	Valssihiomon prosessinohjausjärjestelmä

1 JOHDANTO

Opinnäytetyö on tehty Outokumpu Oyj:n IT-organisaatiolle. Tornion kuumavalssaamolla on käytössä lukuisia eri prosessipaikoille ja eri toimintoihin räätälöityjä tehdasjärjestelmiä, joiden ylläpidosta ja kehitystyöstä vastaa pääosin Outokummun IT-organisaatio.

Kuumavalssaamolla tehdasjärjestelmien historia alkaa jo vuodesta 1987, jolloin linja on käyttöönotettu. Tekniikan kehittyminen on tuonut yhä selvemmin esille sen, että nykypäivänä tietojärjestelmien merkitys on entistä kriittisempää yrityksen liiketoiminnassa. Nykytekniikka tarjoaa suuren mahdollisuuden tukea liiketoimintaa, mutta samalla myös uhan. Luotaessa automatisoituja toimintoja ja laajoja integroituja tietojärjestelmiä rakennetaan samalla monimutkaistuvaa ja hajautuvaa kokonaisuutta.

1.1 Työn tavoitteet ja rajaus

Opinnäytetyön tavoitteena on kartoittaa Tornion kuumavalssaamon IT-palveluun kuuluvien ja vielä kuulumattomien järjestelmien nykytilanne ja tehdä riskianalyysi niiden pohjalta. Riskianalyysin tavoitteena on tunnistaa kriittisimmät tehdasjärjestelmät, tehdä suunnitelmat havaittujen riskien ehkäisemiseksi ja luoda IT-palveluista kehityssuunnitelma seuraavaksi neljälle vuodelle.

Työstä on rajattu pois toimenpide-ehdotusten varsinainen toteuttaminen. Lisäksi yhtenä opinnäytetyön tavoitteena on suunnitella toimintamalleja, joilla voitaisiin parantaa IT-organisaation toimintaa, työn tehokkuutta ja laatua.

1.2 Tutkimusmenetelmät

Tämä opinnäytetyö on toteutettu kvalitatiivisena tutkimusmenetelmänä, jossa on hyödynnetty toimintatutkimuksen tuomaa näkökulmaa. Toimintatutkimus on valittu tutkimusstrategiaksi siksi, että työn tarkoituksena on vaikuttaa toimintaympäristöön ja työssä havaittujen järjestelmäriskien ehkäisyyn. Kvalitatiivinen tutkimusmenetelmä on valittu, koska tarkoitus on löytää konkreettisia parannusehdotuksia. Toisin sanoen

vastauksia ja toimenpide-ehdotuksia on pyritty etsimään kysymykseen ”Miten tehdasjärjestelmät saataisiin tulevaisuudessakin pysymään vähintään yhtä toimintavarmoina ja tukemaan liiketoimintaan ja sen antamia vaatimuksia?”. (Pitkäranta, hakupäivä 7.5.2014.)

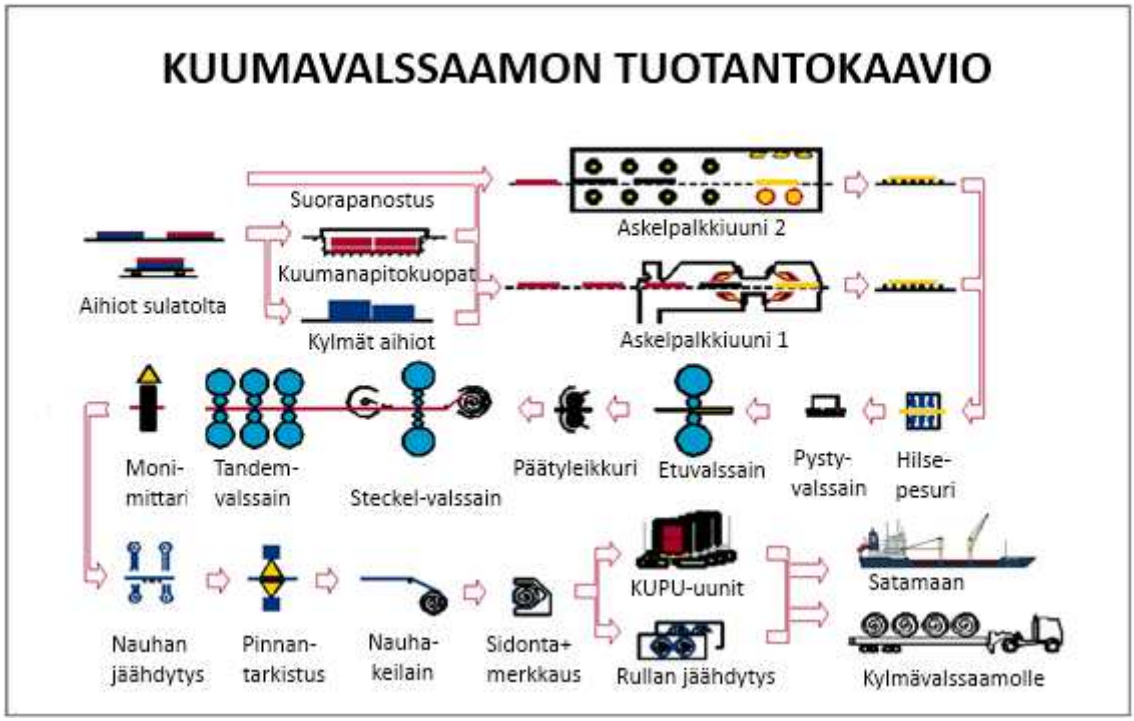
Toiminnan kehittämiseksi on hankittu tietoa keräämällä aineistoa tehdasjärjestelmien olemassa olevasta lähdeaineistosta ja projektien tuottamista dokumenteista. Aineistoa on hankittu myös keräämällä hiljaista tietoa haastattelemalla järjestelmien asiantuntijoita sekä IT-organisaatioista että kuumavalssaamolta.

2 OUTOKUMPU

Outokumpu on monikansallinen metalliteollisuuden yritys, joka työllistää yli 12000 henkilöä yli 30 eri maassa. Outokummun pääliiketoiminta-alueena on ruostumaton teräs, jonka merkittävimmät tuotantolaitokset sijaitsevat Torniossa. Tornion laitokset, ferrokromitehdas, terässulatto, kuumavalssaamo, kylmävalssaamo, satama ja Kemin kromikaivos, muodostavat maailman suurimman ja integroiduimman ruostumattoman terästeollisuuden tuotantoketjun. (Outokummun www-sivut, hakupäivä 11.12.2013.)

2.1 Tornion kuumavalssaamo

Kuvassa 1 näkyy Tornion kuumavalssaamon tuotantokaavio. Seuraavissa kappaleissa on esitelty tuotantolinjan eri prosessipaikat.



Kuva 1. Kuumavalssaamon prosessikaavio (Outokummun www-sivut, hakupäivä 11.12.2013.)

2.1.1 Aihiovarasto ja askelpalkkiuunit

Teräsaihiot tulevat terässulatolta joko rullarataa pitkin tai aihiojunalla kuumavalssaamolle. Kuumavalssaamolla aihiot panostetaan suoraan askelpalkkiuuneihin tai varastoidaan lämpöeristettyihin kuumakuoppiin tai kylmävarastoon.

Askelpalkkiuuneissa aihiot kuumennetaan noin 1270 °C loppulämpötilaan. Uunien polttoaineena käytetään ferrokromitehtaalta talteen otettua häkäkaasua sekä propaania. Askelpalkkiuuneja on kaksi kappaletta, vuonna 1987 käyttöönotettu APU1, jonka maksimikapasiteetti on 120 t/h ja vuonna 2002 käyttöönotettu APU2, jonka maksimikapasiteetti on 250 t/h. Kun aihiot on saatu hehkutettua tavoitelämpötilaan, ne siirretään uunista valssauslinjalle. (Outokummun intranet -sivut, hakupäivä 11.12.2013.)

2.1.2 Etuvalssain

Aihion päältä pestään epäpuhtaudet pois hilsepesurilla ennen etuvalssauksen alkamista. Etuvalssaimella terässulaton 1-linjalla valettu 165 mm tai 2-linjan 185 mm paksu aihio valssataan noin 20–25 mm paksuiseksi esinauhaksi. Tämä tapahtuu viidellä edestakaisella pistolla, jonka aikana pystyvalssit estävät esinauhan liiallisen leviämisen. Valssausnopeus on maksimissaan 6,6 m/s. (Outokummun intranet -sivut, hakupäivä 11.12.2013.)

2.1.3 Nauhavalssain

Nauhavalssain on Steckel-valssain, jossa nauhaa ajetaan valssien välistä 3-7 pistoa riippuen kuumanauhan tavoitepaksuudesta. Valssausnopeus on maksimissaan 10 m/s, jonka jälkeen kuumanauha ajetaan Tandem-valssaimelle, joka koostuu kolmesta valssituolista. Tandem-valssain valssaa nauhan lopulliseen tavoitepaksuuteen, missä valssausnopeus on maksimissaan 18 m/s. (Outokummun intranet -sivut, hakupäivä 11.12.2013.)

2.1.4 Nauhakelain ja rullavarasto

Nauha- ja tandemvalssainten jälkeen kuumanauha ajetaan nauhakelaimelle. Ennen nauhakelainta kuumanauha jäähdytetään laminaarijäähdytyksellä 1000 °C:sta noin 600–700 °C:een. Nauhakelain kelaa kuumanauhan rullaksi, jonka jälkeen rulla merkataan, punnitaan ja sidotaan. Valmis rulla siirretään automaattinostureilla joko kuivavarastoon ja vesivarastoon jäähtymään. Kuivavarastossa rulla jäähtyy lähetyskelpoiseksi noin 24 tunnissa, vesivarastossa jäähtyminen kestää noin kahdeksan tuntia. Jäähtyneet rullat kuljetetaan joko kylmävalssaamolle jatkokäsittelyyn tai suoraan satamaan ja sieltä asiakkaalle. (Outokummun intranet -sivut, hakupäivä 11.12.2013.)

2.1.5 Kupu-uunit

Kupu-uunikäsittelyn tavoitteena on teräksen mikrorakenteen homogenisointi, mikä mahdollistaa tiettyjen ferriittisten teräslaatujen valmistuksen. Rullat siirretään automaattinosturilla kellistinkuljettimelle, joka kaataa rullan vaaka-asentoon. Rullat siirretään manuaalinosturilla alustoille, johon mahtuu maksimissaan neljä rullaa, riippuen rullan leveydestä ja mahdollisesta teleskooppisuudesta. Rullien väliin pinotaan väliarinat helpottamaan pinoamista ja parantamaan kaasunkiertoa käsittelyssä. Prosessin aikana rullia hehkutetaan vetyatmosfäärissä noin vuorokausi, minkä jälkeen rullat jäähdytetään typpiatmosfäärissä. Lopuksi rullat puretaan alustalta siirtämällä ne yksitellen takaisin kellistinkuljettimelle, missä rullat nostetaan takaisin pystyasentoon ja siirretään varastoon jäähtymään automaattinosturilla. Tornion kuumavalssaamolla neljä ensimmäistä kupu-uunia otettiin käyttöön vuonna 2007 ja viides vuonna 2011. (Outokummun intranet -sivut, hakupäivä 11.12.2013.)

2.1.6 Valssihiomo

Kaikki valssauslinjan valssit hiotaan valssihiomossa. Valssihiomossa on neljä hiomakonetta, joista kaksi vanhempaa, hiomakone 1 ja 2, ovat saksalaisen Herculesin toimittamia ja uudemmat, hiomakone 3 ja 4, italialaisen Poiminin toimittamia. (Outokummun intranet -sivut, hakupäivä 11.12.2013.)

Hiomakone 1:llä hiotaan etuvalssaimen työ- ja tukivalsseja, koska hiomakone on tehokkaampi kuin hiomakone 2. Hiomakone 2:lla hiotaan pääasiassa nauhavalssaimen työ- ja välivalsseja. Pominin toimittamalla hiomakone 3:lla hiotaan tuotantotilanteesta riippuen nauhavalssaimen tuki-, väli- ja työvalsseja sekä tandemvalssainten työ- ja tukivalsseja. Hiomakone 4:lla hiotaan tandemvalssaimen työvalsseja. Hiomakoneet 3 ja 4 toimivat automaattinosturin alueella, joka siirtää valsseja varastoon, hiomakoneille ja valssiensiirtovaunuun. (Outokummun intranet -sivut, hakupäivä 11.12.2013.)

3 RISKIENHALLINTA

Riskienhallinta on jatkuvatoiminen prosessi, jolla pyritään turvaamaan toimintaympäristö siltä uhkaavilta vaaroilta ja ongelmilta sekä välttämään ja pienentämään näistä aiheutuneita vahinkoja. Riskienhallinnan ydinajatus on taata toimintaympäristön, esimerkiksi yrityksen toiminnan jatkuvuus riskien toteutumisesta huolimatta. (Kuusela & Ollikainen 2005, 155.)

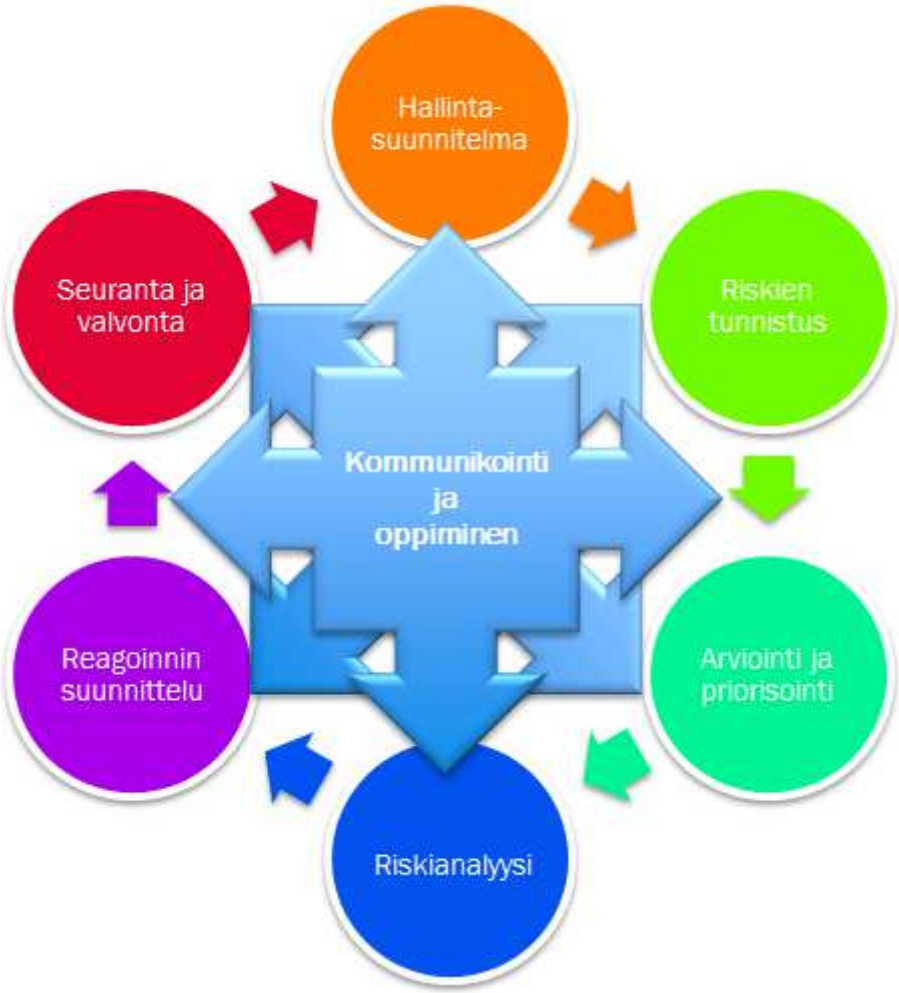
Kuvassa 2 on esitelty esimerkki kuusivaiheisesta riskienhallintaprosessista. Prosessin ensimmäinen vaihe on riskien tunnistaminen. Riskien tunnistus kertoo seikkaperäisemmin havaittujen riskien painopisteet, joka helpottaa riskienhallinnan kohdistamista oikeisiin asioihin. Kun riskit on tunnistettu, seuraavana vaiheena on niiden arviointi ja priorisointi. Riskien arviointi perustuu pitkälti olemassa olevaan kokemukseen ja asiantuntemukseen, mutta silti riskien yliarviointia tulisi välttää. Yliarviointi voi johtua esimerkiksi siitä, että riskeistä puhutaan ja kirjoitetaan paljon. Tarjottava informaatio kasvattaa riskitietoisuutta, joka voi aiheuttaa yliarviointia, mutta aliarviointia taas paljon harvemmin. (Kuusela & Ollikainen 2005, 155.)

Riskien arvioinnin ja tunnistamisen jälkeen suoritetaan määrällinen riskianalyysi, jonka tarkemmat vaiheet on kuvattu kappaleessa 3.5. Riskien analysointi antaa pohjan myös riskitilanteiden seurannalle ja helpottaa muutosten ennakointia ja niihin reagointia. Riskien analysoiminen antaa myös perustan tärkeille päätöksentekotilanteille. (Kuusela & Ollikainen 2005, 233.)

Riskien seuranta- ja valvontavaiheessa toteutuneista ja toteutumattomista riskeistä raportoidaan ja luodaan samalla varasuunnitelmia toteutuneiden riskien välttämiseksi tulevaisuudessa. Hyvä riskien valvonta ja seuranta tuottaa tietoa, joka myös auttaa päätöksenteossa, ennen riskin toteutumista. (Risk monitoring and control. Hakupäivä 7.5.2014.)

Näiden edellä mainittujen vaiheiden pohjalta luodaan riskienhallintasuunnitelma. Kuten kuvasta 2 ilmenee, riskienhallintasuunnitelma antaa pohjan seuraavalle riskien tunnistusvaiheelle. Kaikkea riskinhallintaprosessin vaiheita yhdistää prosessin keskeinen osa, eli kommunikointi ja oppiminen. Jatkuvatoiminen prosessi kartuttaa

tiedon ja osaamisen määrää, joka tulisi välittää toimintaympäristön jokaiselle sidosryhmän edustajalle. Yritysmaailmassa tämä tarkoittaa, asiantuntijoita, esimiehiä sekä yrityksen johtoa. (Kuusela & Ollikainen 2005, 233.)



Kuva 2. Riskienhallintaprosessi (Malmén & Wessberg. Hakupäivä 7.5.2014.)

3.1 Riskin määrittely

Sana riski tulee latinan sanasta ”risicare”, joka tarkoittaa karikon kiertämistä. Italiaksi kyseinen sana tarkoittaa uskaltamista. Ihmisten ja yritysten elämään kuuluu epävarmuus, joka johtuu tietämättömyydestä tulevista tapahtumista, jotka voivat olla kielteisiä tai myönteisiä. Myös riskien toteutumiseen liittyy aina epävarmuus ja toteutuessaan ne sisältävät odotuksia, jotka määrittelevät millaisena tapahtuma koetaan. Tapahtuman laajuus ja sen arvioitu todennäköisyys liittyvät oleellisesti riskin merkityksellisyyteen. (Kuusela & Ollikainen 2005, 15–31.)

Eri tieteenaloilla sanalla on useita käyttötarkoituksia ja merkityksiä. Seuraavat viisi käsitettä riskistä ovat yleisimmin käytössä:

1. ei toivuttu tapahtuma, jonka tapahtuminen on epävarmaa
2. seuraus ei toivotusta tilanteesta, jonka tapahtuminen on epävarmaa
3. todennäköisyys ei halutulle tilanteella, jonka tapahtuminen on epävarmaa
4. tilastollinen odotusarvo ei halutulle tilanteelle, jonka tapahtuminen on epävarmaa
5. päätös, joka on tehty ottaen huomioon tiedetyt tosiasiat.

Seuraavassa listassa on esimerkkejä tupakoinnista, jonka riskiä on havainnollistettu yllämainituissa käsitteissä:

1. keuhkosyöpä on yksi suurimmista tupakoinnin riskeistä
2. tupakointi on merkittävin terveysriski teollisuusmaissa
3. tupakoitsijan odotettu elinikä lyhenee tupakointiin liittyvien sairauksien vuoksi 50 prosentilla
4. Tilastollisesti tupakointi on pääsyy 22 prosentissa syöpäkuolemissa
5. Aloitan tupakoinnin. (Stanford Encyclopedia of Philosophy. Hakupäivä 7.5.2014)

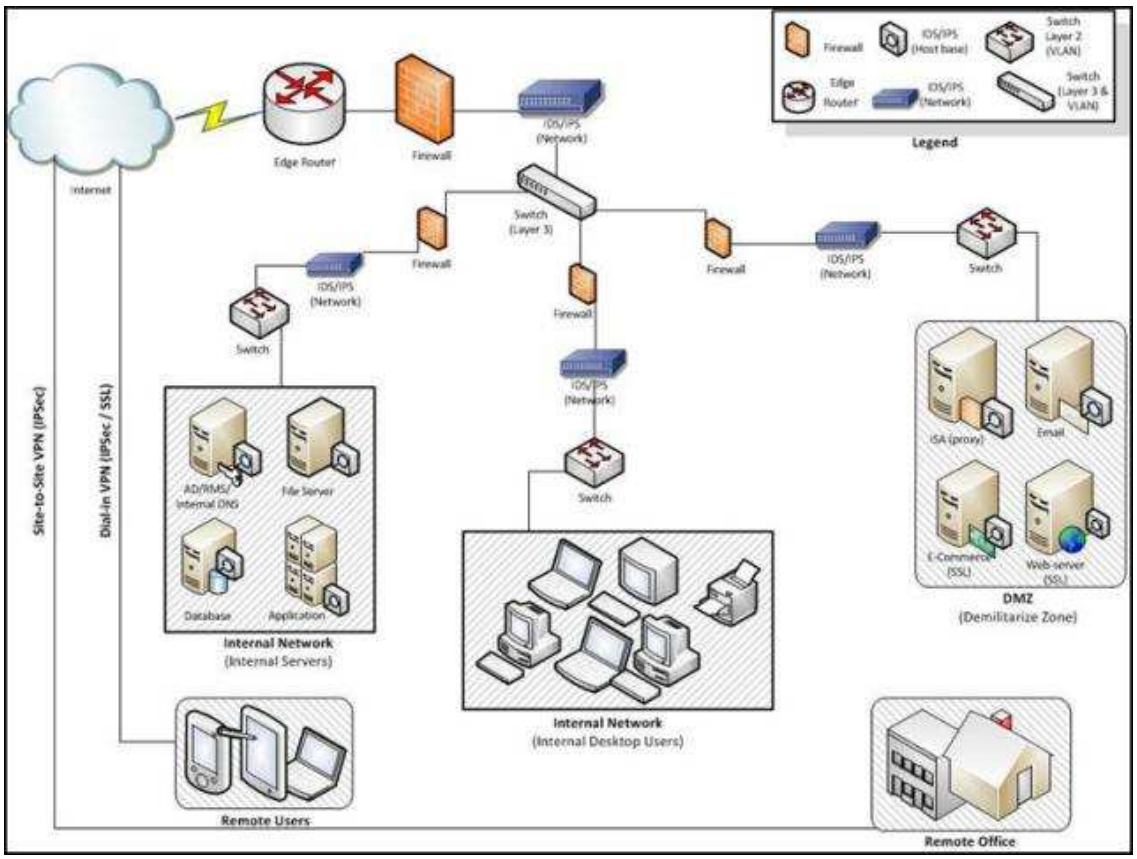
3.2 Tietojärjestelmien riskienhallinta

IT-järjestelmien merkitys liiketoiminnalle on kasvanut merkittävästi viime vuosina ja yhä useampi liiketoiminta on riippuvainen järjestelmistä. Tämän vuoksi on tärkeä selvittää, mistä järjestelmistä kukin prosessi on riippuvainen ja kuinka eri järjestelmät ovat riippuvaisia toisistaan. Järjestelmien riippuvuussuhteissa pitäisi aina tarkastella isompaa järjestelmäkokonaisuutta, koska riskinä voi olla, että itsenäisenä tarkasteltu vähemmän tärkeä järjestelmä voikin olla tukijärjestelmä toiselle tärkeämmälle tai kriittisemmälle järjestelmälle, jolloin sen tärkeysaste prosessin näkökulmasta vääristyy. (Iivari & Laaksonen 2009, 114.)

Jokainen tietojärjestelmä on jollain tavalla haavoittuvainen. Niitä voivat uhata esimerkiksi erilaiset hyökkäykset organisaation sisä- ja ulkopuolelta, laitevahingot ja käyttäjävirheet. Seuraavissa kappaleissa on esitelty viisi tietojärjestelmien osa-aluetta ja kuvattu eri osa-alueisiin kohdistuvia riskejä ja niiden hallintaa. (Iivari & Laaksonen 2009, 114.)

3.2.1 Infrastruktuuri

Tietojärjestelmien infrastruktuurilla ymmärretään pääsääntöisesti kaikkia fyysisiä asioita, jotka liittyvät tietojärjestelmien toimintaedellytyksiin. Näitä ovat tietoliikenneverkko, palvelimet sekä työasemat. Kuvassa 3 ilmenee esimerkki yrityksen IT-infrastruktuurista. (Kuusela & Ollikainen 2005, 251–260.)



Kuva 3. Esimerkki organisaation IT-infrastruktuurista (Modeling Secure Network Architecture, hakupäivä 18.1.2014.)

Tietoliikenneverkko on välttämätön yritykselle, jonka varaan kaikki IT-palvelut rakennetaan ja jolla mahdollistetaan palveluiden käyttö. Tietoliikenneverkosta on pidettävä hyvää huolta monella tavalla, koska verkko antaa yritykselle mahdollisuuden ja samalla myös uhan. Normaalisti yrityksen verkko suojataan ulkomaailmalta palomuureilla, johon määritellään sallitut tietoliikenneprotokollat sekä yrityksestä ulkomaailmaan näkyvät palvelut. Sisäverkko jaetaan myös aliverkkoihin, jotka suojataan omilla palomuureillaan. Näin tietoliikenneverkon suojaus saadaan kerrostettua, mikä tekee verkkoon luvattomasta tunkeutumisesta vaikeampaa. (Kuusela & Ollikainen 2005, 251–260; Iivari & Laaksonen 2009, 182–184.)

Tietoliikenneverkon riskien juurisyyt juontavat verkon käytettävyyden vaatimuksista. Verkon tietoturvan tulee olla korkealla tasolla ja verkon tulee olla aina käytössä. Lisäksi verkon kapasiteetin pitää riittää myös uusille käyttötavoille. (Kuusela & Ollikainen 2005, 251–260.)

Organisaation aliverkkojen ympärille asennetaan palvelimet, jotta niiden tarpeettoman laajalle näkyminen saataisiin estettyä. Palvelin on tietokone, joka tarjoaa siinä ajettavien ohjelmistojen välityksellä erilaisia palveluja muille ohjelmille ja käyttäjille. Organisaatiossa voi olla erilaisia palvelimia useita kymmeniä jopa useita satoja ja niitä pystytään aina, kun tarve ilmenee. Palvelimien riskit kohdistuvat pääosin niiden varalaitejärjestelyihin, ylläpitoon ja tietoturvaan. Palvelimien määrän ja niiden kirjon kasvaessa ylläpito nousee avainasemaan. (Kuusela & Ollikainen 2005, 251–260; Iivari & Laaksonen 2009, 185–186.)

Varmistusjärjestelmät liittyvät oleellisena osana palvelimien vikasietoisuuteen ja riskienhallintaan. Niillä turvataan tietojen saatavuus tietojärjestelmien häiriötilanteissa, kuten laiterikkojen aiheuttamissa tieto-omaisuuden katoamisissa ja rikkoutumisissa. Varsinkin korkean käytettävyyden ympäristöt pitäisi suunnitella ja rakentaa siten, että vikatilanteissa palvelut olisivat mahdollisimman nopeasti jälleen käytettävissä. Palvelimet, joilta vaaditaan korkeaa käytettävyyttä, pitäisi varmentaa esimerkiksi kahdennuksella, klusteroinnilla tai virtualisoinnilla. (Iivari & Laaksonen 2009, 167–176.)

Kahdennuksella tarkoitetaan palvelinlaitteiden mekaanisten osien ja myös ohjelmistojen monistamista. Kahdennus ei tarkoita pelkästään varmuuskopiointia, vaan tekniikkaa jonka avulla kriittiset tiedot ja toiminnot ovat käytössä sellaisenaan. Jos käytössä oleva palvelin vikaantuu, se voidaan korvata identtisellä varakoneella joko automaattisesti ja manuaalisesti. Palvelimien kahdennus on yleensä helpoin tapa turvata järjestelmän käytettävyys, mikäli vain hyväksytään siitä aiheutuvat käyttökatkokset. Kahdennuksen huonoja puolia ovat varakoneen tai varakoneiden pitäminen ajan tasalla, jos käytössä olevaan palvelimeen tehdään päivityksiä. (Iivari & Laaksonen 2009, 167–176.)

Klusteroinnilla tarkoitetaan palveluiden ja palvelimien monistamista siten, että palvelimien sisältämä tieto ja toiminnallisuudet on varmennettu reaaliaikaisesti ja kahdensuuntaisesti. Klusterointi eroaa kahdennuksesta siinä, että klusterissa eri palvelimet toimivat yhtä aikaa ja jakavat palvelun kuormaa. Mikäli jokin klusterin palvelimista vikaantuu, palvelut jakaantuvat muille klusterissa oleviin palvelimiin ja näin loppukäyttäjä ei välttämättä näe mitään vikatilannetta. Kun vikaantunut palvelin on

taas käytettävissä, palvelut ja kuormitus jakaantuvat uudestaan koko laitekokoonpanolle. (Iivari & Laaksonen 2009, 167–176.)

Virtualisoinnilla tarkoitetaan tekniikkaa, missä yhdessä fyysisessä laitteessa ajetaan yhden käyttöjärjestelmän sijasta useita virtuaalipalvelimia, joissa kukin käyttää itsenäisesti omaa käyttöjärjestelmäänsä. Tyypillisesti virtualisoinnilla haetaan kustannussäästöjä ja fyysisen laitekannan vähentämistä. (Iivari & Laaksonen 2009, 167–176.)

Työasemat ovat laitteita, joilla käyttäjä hyödyntää verkossa olevia palveluja. Työasema voi olla joko kiinteä työpöydällä oleva tietokone, kannettava, taulutietokone tai kännykkä. Työaseman koon pienentyessä, niiden katoamis- ja varkausriskit kasvavat. Tämän vuoksi työasemissa ei saisi olla näkyvillä yrityksen nimeä tai logoa. (Kuusela & Ollikainen 2005, 251–260.)

Ylläpidon kannalta ongelmana on työasemien käyttäjien jakaminen pääkäyttäjään ja peruskäyttäjään. Yleensä työaseman käyttäjällä on peruskäyttäjän oikeudet, minkä vuoksi työaseman käytön joustavuus saattaa kärsiä, koska työasemia ylläpitävä henkilöstö hoitaa kaikki työaseman asetukset ja asennukset. Toisaalta tämä parantaa työasemien vakaata käyttöä ja vähentää virhemahdollisuuksia ja tietoturvariskejä. Jokaisessa verkkoon liitetyssä työasemassa pitäisi olla virustorjuntaohjelmisto estämässä mm. haittaohjelmien pääsyä yksittäiseen työasemaan ja sitä kautta muihin samassa tietoliikenneverkossa oleviin laitteisiin. (Kuusela & Ollikainen 2005, 251–260.)

3.2.2 Sovellukset

Infrastruktuurin toiminta liittyy merkittävästi sovellusten toimintaan, sillä sovellukset sijoittuvat tietojärjestelmien perusinfrastruktuurin ja tietojärjestelmäpalveluiden väliin. Sovellusten avulla tuotetaan käyttäjien tarvitsemat toiminnallisuudet ja palvelut. Sovelluksiin kohdistuvat riskit perustuvat käytettävyyteen, toimivuuteen sekä niiden muutosten hallintaan. (Iivari & Laaksonen 2009, 189–201.)

Monilla organisaatioilla sovellukset ovat pitkälti räätälöityjä heidän omiin tarpeisiinsa. Sovellusten jatkuvuuden varmistaminen on vaikeaa, jos asiakas ei omista sovelluksen lähdekoodeja ja sovelluksen toimittanut yritys ei ole halukas tai kykenevä tukemaan tai kehittämään sitä. Liiketoiminnalle kriittisissä räätälöidyissä sovelluksissa tulisi pyrkiä siihen, että sovellusten lähdekoodit ovat asiakkaan omistuksessa. Tällä pystytään varmistamaan sovelluksen toiminta ja jatkuvuuden turvaaminen. Jos yritys on hankkimassa uutta järjestelmää, tulisi tämä vaatimus esittää jo tarjouspyynnössä. (Iivari & Laaksonen 2009, 189–201.)

Sovellusten muutoshallinnassa testauksella on merkittävä rooli myös riskienhallinnan näkökulmasta. Testaus on yksi sovelluskehityksen vaiheista, joka toimii samalla yhtenä laadunvalvonnan osa-alueena. Testauksen tavoitteena on havaita sovelluksessa ilmeneviä virheitä, jotta ne voidaan korjata, sekä varmistaa, että sovellus toimii oikein ja tarjoaa liiketoiminnan määrittelemät toiminnallisuudet ja vaatimukset. Kaikki testausprosessin aikana löydetyt ja korjatut virheet parantavat käyttöönotettavan version laatua ja pienentävät liiketoimintaan kohdistuvia riskiä. (Tauriainen 2007, 9–10.)

3.2.3 Palveluntarjoajat

ICT-palveluiden ulkoistaminen ja ulkopuolisten palveluntarjoajien käyttö on nykyisin täysin normaalia yritysmaailmassa. Palveluiden ulkoistamisella pyritään saavuttamaan taloudellisia etuja. Laite- ja henkilöstöinvestointeja saadaan vähennettyä sekä liiketoiminnan asettamat tarpeet voidaan ostaa palveluina yritykseltä, jolle kyseiset palvelut ovat pääliiketoimintaa. Palveluiden ulkoistaminen voidaan jaotella esimerkiksi seuraavasti:

- verkkopalvelut
- ohjelmointi
- järjestelmien ylläpito
- laitteistojen ylläpito
- elektroniset liiketoimintaratkaisut
- tietoturva
- loppukäyttäjien tuki, esim. helpdesk

- henkilöstön/käyttäjien koulutus. (Iivari & Laaksonen 2009, 185–188, 217–229.)

Palveluntarjoajasta koituvat riskimahdollisuudet ja ongelmat pohjautuvat lähtökohtaisesti puutteellisesti laadittuihin sopimuksiin. Tällöin ei välttämättä tunneta palvelun tarjoajan resursseja ja kyvykkyyttä. Sopimuksia laadittaessa yrityksen pitäisi huomioida haluttujen palveluiden vaatimustaso ja laatia sopimukset riittävän kattavasti, jotta ongelmatilanteissa olisi selkeät pelisäännöt ja vastuut, eikä tulkinnan varaa jäisi. Esimerkiksi huoltosopimuksissa on oleellista määrittää järjestelmien käytettävyysvaatimusten mukainen huoltopalvelun saatavuus, kuten vasteajat, varaosien saatavuus ja kriittisten palveluiden monitorointi, koska varsinkin monista mekaanisissa laitteissa on tiedossa niiden todennäköinen vikaantumisaika tai valmistajan suosittelema käyttöaika. (Iivari & Laaksonen 2009, 185–188, 217–229.)

3.2.4 Strategiset riskit ja tulevaisuuden uhat

Tietojärjestelmien strategiset riskit ja tulevaisuuden uhat kohdistuvat niiden elinkaaren hallintaan. Yrityksellä tulisi olla selkeä kuva laitteistojen ja järjestelmien käytön ajallisesta pituudesta sekä valmistajien antamien huoltotukien saatavuudesta. Esimerkiksi Microsoft on ilmoittanut lopettavansa Windows XP-käyttöjärjestelmän tuen 8.4.2014. Tämä tarkoittaa sitä, että Windows XP:hen ei saa enää esimerkiksi tietoturvapäivityksiä tuon jälkeen. Tietoturvariskien välttämiseksi Microsoft suosittelee käyttöjärjestelmän päivittämistä uudempaan tai hankkimaan uuden tietokoneen, mikäli uudempi käyttöjärjestelmä ei työasemassa toimi.

Yrityksille räätälöityjen järjestelmien osalta tämä saattaa vaikuttaa siihen, että järjestelmä ei välttämättä toimikaan uudessa käyttöjärjestelmässä. Jäljelle jää siis kaksi vaihtoehtoa. Päivittää järjestelmä toimimaan tuetussa käyttöjärjestelmässä tai ajaa järjestelmää vanhassa ympäristössä tiedostaen mahdolliset tietoturvariskit. (Iivari & Laaksonen 2009, 217–229.; Windows XP:n tuki on päättymässä, hakupäivä 20.1.2014.)

3.2.5 Käyttäjät

Myös järjestelmien ja sovellusten käyttäjät voidaan luokitella yhdeksi tietojärjestelmiin kohdistuvaksi riskiksi. Käyttäjien toimesta voi aiheutua tahatonta tietovuotoa sähköpostiviesteissä tai puhelimessa, mutta tietovuodot voivat olla myös tahallisia. Tämän vuoksi on oleellista huolehtia, että jokaisen käyttäjän tarjolla olevat tiedot ja toiminnot vastaavat hänen työtään. Tietovuotojen lisäksi käyttäjät voivat tahattomasti käyttää järjestelmiä ja ohjelmistoja siten, että siitä koituu harmia. Yleensä tämän syynä on puutteellinen koulutus tai ohjeistus. (Kuusela & Ollikainen 2005, 244–250.)

3.3 Riskianalyysi

Riskit on arvioitava säännöllisesti. Tämä olisi hyvä tehdä vuosittain tai aina kun toimintaympäristössä tapahtuu merkittäviä muutoksia. Riskianalyysiä tehdessä pitää ymmärtää uhkien aiheuttajat, jotka kohdistuvat yrityksen prosesseihin ja tietojärjestelmiin. Uhkien aiheuttajia voivat olla muun muassa oma henkilöstö, ulkopuoliset toimijat, järjestelmien ja laitteiden tekniset virheet tai vikaantumiset. (Iivari & Laaksonen 2009, 117–137.)

Riskianalyysiin on olemassa monia malleja, esimerkiksi haavoittuvuusanalyysi ja erilaiset riskianalyysimatriisit. Mallit tarjoavat pohjan ja etenemissuunnitelman riskianalyysin tekemiseen, mutta pohjimmiltaan ne eivät vaikuta varsinaisen riskianalyysin sisältöön. Mallin valinnasta riippumatta, riskianalyysiin kuuluu yleensä seuraavat vaiheet:

- tarkasteltavien kohteiden arvo liiketoiminnalle
- riskien tunnistaminen ja niiden vakavuuden määrittely
- ennakointi ja ehkäisevien toimenpiteiden määrittely
- toimintasuunnitelman laatiminen riskien toteutumisen varalta. (Iivari & Laaksonen 2009, 117–137.)

Riskianalyysin ensimmäisessä vaiheessa pyritään tunnistamaan ja arvioimaan niiden toimintojen arvo, herkkyys ja kriittisyys, joita tunnistettavat uhat uhkaavat. Erityisen

tärkeää on tunnistaa liiketoiminnan kannalta tärkeimmät ja kriittisimmät toiminnot. (Iivari & Laaksonen 2009, 117–137.)

Seuraavana vaiheena on riskien tunnistaminen. Tavoitteena luoda kattava luettelo riskeistä, jotka uhkaavat tarkasteltavia kohteita. Riskien tunnistaminen on oleellinen osa riskianalyysiä, koska tunnistamattomia riskejä ei voi hallita. Riskien tunnistamisella tarkoitetaan riski- ja uhkatilanteiden kartoittamista erilaisia menetelmiä käyttäen. Yleisempiä menetelmätapoja ovat historiatieto sekä tietoon ja asiantuntemukseen perustuvat näkemykset ja mielipiteet. (Iivari & Laaksonen 2009, 117–137.)

Riskien tunnistamisen jälkeen arvioidaan niiden vakavuutta ja seurausvaikutuksia. Taulukossa 1 on esimerkki, kuinka riskit voidaan jakaa neljään eri tasoon. Valittuun riskilukuun vaikuttaa pitkälti asiantuntemukseen perustuvat näkemykset ja kokemukset.

Taulukko 1. Riskien vakavuuden määrittely (Iivari & Laaksonen 2009, 117–137.)

Riskiluku	**Riskin kuvaus**
0	Ei riskiä
1	Matala riksi
2	Keskimääräinen riski
3	Korkea riski

Taulukossa 2 on esimerkki, kuinka riskiluku saadaan johdettua määrittelemällä riskin todennäköisyys ja vahinkoseuraus. Taulukoissa 1 ja 2 on käytetty samanlaista 4-portaista riskinluvun luokittelua.

Taulukko 2. Esimerkki 4x4 vahinkoseuraus-todennäköisyys riskimatriisista (Occupational Health and Safety Risk Assessment Sample 4x4 Risk Matrix, hakupäivä 5.4.2014.)

VAHINKOSEURAUS	TODENNÄKÖISYYS: 1 - Harvinainen	2 - Epätodennäköinen	3 - Mahdollinen	4 - Todennäköinen
4 - Katastrofaalinen	4	8	12	16
3 - Merkittävä	3	6	9	12
2 - Kohtalainen	2	4	6	8
1 - Pieni	1	2	3	4

Riskianalyysin seuraavassa vaiheessa pyritään tunnistamanaan kustannustehokkaat tavat ja toimet, joilla olisi mahdollista poistaa, vähentää tai hallita riskejä. Näitä voivat olla esimerkiksi organisaation uudet tai päivitetyt prosessit tai tekniset kontrollit. Tämän jälkeen toimenpiteet suhteutetaan riskien suuruuteen. Toimenpiteet voidaan karkealla tasolla jakaa omiin riskienhallintatoimenpiteisiin tai riskin siirtämiseen. Riskienhallintatoimenpiteitä ovat riskin pitäminen tai hyväksyminen, riskin pienentäminen, riskin poistaminen, riskin välttäminen ja riskin siirtäminen. Taulukossa 3 on kuvattu esimerkkejä erilaisten riskien hallintatoimenpiteiksi. (Iivari & Laaksonen 2009, 117–137.)

Taulukko 3. Toimenpiteet eritasoisille riskeille (Iivari & Laaksonen 2009, 117–137.)

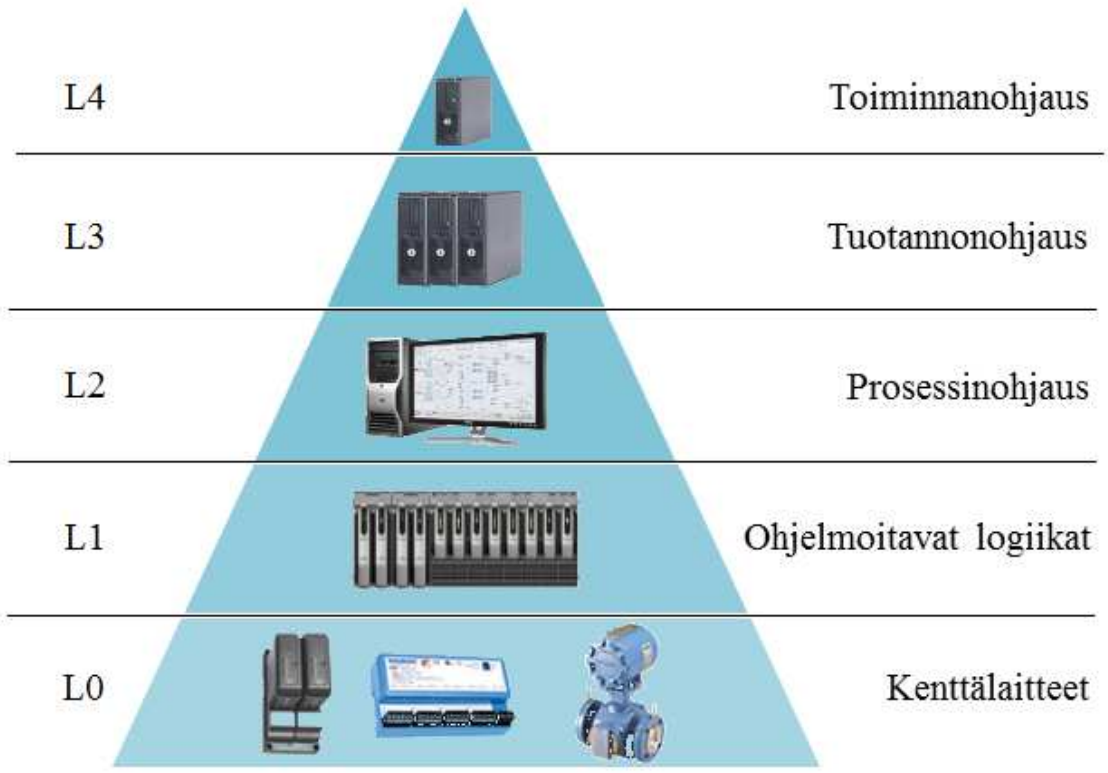
Riskiluku	Riskin kuvaus	Toimenpiteet
0	Ei riskiä	Ei toimenpiteitä.
1	Matala riksi	Ei merkittäviä toimenpiteitä. Riskiä tulee mahdollisuuksien mukaan poistaa tai pienentää. Seurattava, että riski pysyy hallinnassa.
2	Keskimääräinen riski	Tulee kohtuulliseksi katsotun ajan kuluessa ryhtyä toimenpiteisiin riskin poistamiseksi tai pienentämiseksi hyväksyttävälle tasolle
3	Korkea riski	Ryhdyttävä aktiivisiin toimenpiteisiin riskin poistamiseksi tai pienetämiseksi hyväksyttävälle tasolle.

Riskianalyysin tuloksena syntyy esimerkiksi taulukko, johon listattu kaikki organisaation toimintaa uhkaamat riskit, niiden vaikutukset sekä niihin varautuminen. Tämän lisäksi riskianalyysissä on kyse myös asioiden dokumentoinnista, minkä avulla pystytään viestimään yrityksen riskienhallintaan liittyviä tavoitteita ja toimenpiteitä.

4 JÄRJESTELMÄSELVITYS

Tornion kuumavalssaamon tehdasjärjestelmät voidaan ISA-95-standardin mukaan viiteen eri tasoon, jotka on esitelty kuvassa 4. Ylin taso (L4) käsittää toiminnanohjausjärjestelmät, joissa käsitellään esimerkiksi tilauksia, kirjanpitoa ja laskutusta. Tuotannonohjaustasolla (L3) olevat järjestelmät ovat koordinoinnista vastaavia ohjelmistoja, jotka integroivat automaation ja toiminnanohjauksen. (Manufacturing Operations Management, hakupäivä 5.4.2014.)

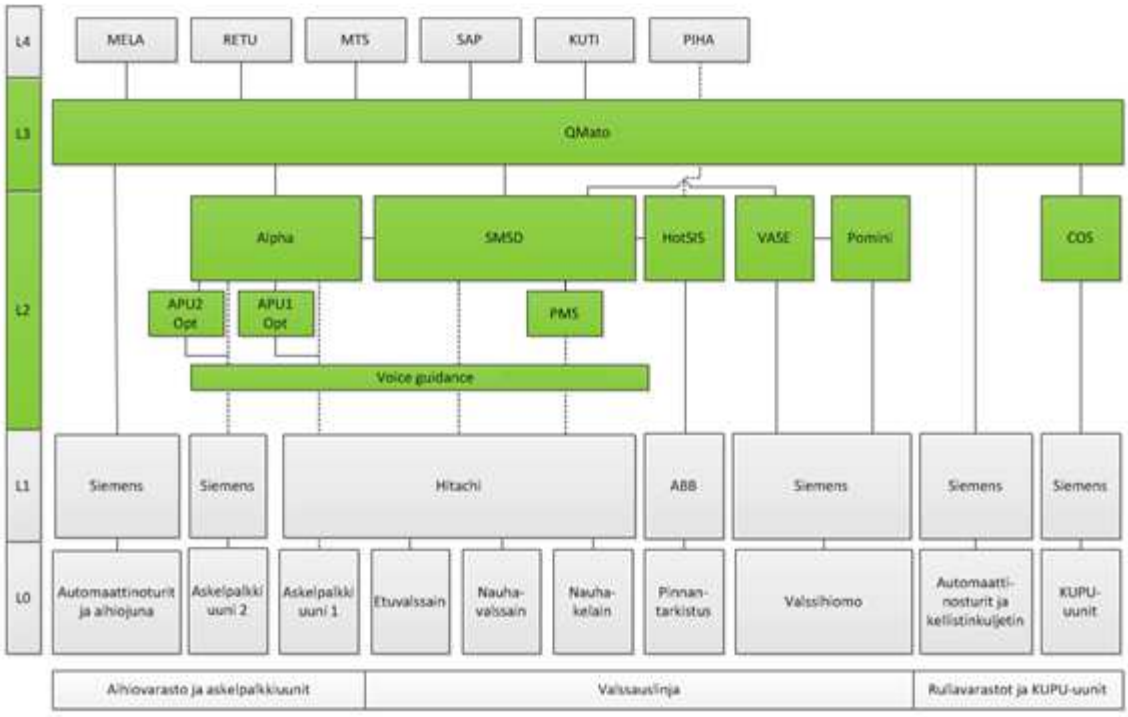
Tuotannonohjausjärjestelmät keräävät prosessinohjausjärjestelmiltä (L2) tietoa prosessin vaiheista ja nimensä mukaisesti ohjaavat tuotantoa. Prosessinohjausjärjestelmät lähettävät ohjausparametrit ohjelmoitaville logiikoille (L1), joiden tehtävänä on ohjata prosessipaikan kenttälaitteita esimerkiksi moottoreita, venttiilejä ja pumppuja. (Manufacturing Operations Management, hakupäivä 5.4.2014.)



Kuva 4. Järjestelmätasot (Suomen automaatioseura 2007)

4.1 Kuumavalssaamon tehdasjärjestelmät

Kuvassa 5 on esitelty kuumavalssaamon tehdasjärjestelmät kuvan 4 mukaisella järjestelmäjaottelulla. Tässä järjestelmäselvityksessä käsitellään vain prosessin- ja tuotannonohjaustasoihin kuuluvia järjestelmiä. Liitteessä 1 on esitelty yksityiskohtaisemmin järjestelmien arkkitehtuurikuvaukset.



Kuva 5. Kuumavalssaamon tehdasjärjestelmät

4.1.1 Tuotannonohjaus

Tornion terässulatolla ja kuumavalssaamolla on yhteinen tuotannonohjausjärjestelmä QMato, joka on käyttöönotettu vuonna 2002. QMato saa sulatustilaukset MTS:ltä ja lähettää prosessinohjausjärjestelmille tuotteiden perustiedot muun muassa teräslajin, sulatuksen analyysitietoja prosessin eri vaiheista ja asiakasvaatimukset. Sulakäsittelyssä QMato pääasiassa vain vastaanottaa käsittelyn tietoja prosessinohjausjärjestelmiltä.

QMatossa on myös varastonhallintatoiminnallisuudet sekä aihio- että rullakäsittelyyn. Terässulaton 1-linjan aihiovarastossa, kuumavalssaamon aihiovarastossa ja rullavarastoissa on automaattinosturit, jotka kommunikoivat suoraan QMaton kanssa.

Tämä toteutusmalli (L3 ↔ L1) poikkeaa hieman muista järjestelmäintegroinneista, koska automaattinostureilla ei ole omaa prosessinohjausjärjestelmää. Toisaalta varastonhallinnan kannalta tämä toteutusmalli on todettu hyväksi, koska erillistä sanomaliikennerajapintaa ja muuta toiminnallisuutta ei tarvitse rakentaa tuotannonohjausjärjestelmän ja varastonhallintajärjestelmän välille. Aihio- ja rullalogistiikan hallinta ovat yksi QMaton kriittisimpiä toimintoja.

4.1.2 Prosessinohjaus

Kuumavalssaamolla on viisi varsinaista prosessinohjausjärjestelmää. Askelpalkkiuunien alueella Alpha, valssauslinjalla SMSD, valssihiomossa VASE ja Pomini sekä kupu-uunialueella COS. Tämän lisäksi muita tukijärjestelmiä ovat askelpalkkiuunien optimointijärjestelmät (APU1-optimointi ja APU2-optimointi), pinnantarkistusjärjestelmä HotSIS sekä valssauslinjan tapahtumista valvomoihin ilmoittava Voice guidance -järjestelmä.

Alpha-järjestelmä on otettu käyttöön vuonna 1997, jolloin se toimi askelpalkkiuunien prosessinohjauksen lisäksi myös koko valssauslinjan prosessinohjausjärjestelmänä. Nimensä järjestelmä on saanut palvelinympäristönsä mukaan. Valssauslinjan toiminnallisuudet on karsittu pois vuonna 2004, jolloin SMSD-järjestelmä on käyttöönotettu. Nykyään Alpha kommunikoi APU-alueen automaatiojärjestelmien Siemensin ja Hitachin (L2 ↔ L1 integraatio) kanssa, molempien APU-optimointijärjestelmien kanssa sekä tuotannonohjausjärjestelmä QMaton kanssa. Palvelinympäristönä toimii edelleen vuonna 1997 käyttöönotettu Digital Alpha 4000.

Molemmilla askelpalkkiuuneilla on yhteisen prosessinohjausjärjestelmän lisäksi omat optimointijärjestelmänsä. Optimointijärjestelmillä on tarkoitus säästää teräsaihioiden hehkutuksessa käytettävän nestekaasun määrää ja ajoittaa aihioiden ulosotto mahdollisimman oikea-aikaiseksi. Askelpalkkiuuni 2:n optimointijärjestelmä on otettu käyttöön vuonna 2002 ja järjestelmän palvelinympäristönä on sama Alpha-palvelin kuin askelpalkkiuunien prosessinohjausjärjestelmällä. APU1-optimointi on otettu käyttöön vuonna 2008 ja sen palvelinympäristönä on Windows 2003 Server. Molemmilla optimointijärjestelmillä on samanlainen laskentamalli ja toimittajana on saksalainen LOI Thermoprocess GmbH.

SMSD- järjestelmä on otettu käyttöön vuonna 2004 Steckel-projektissa. Järjestelmän on toimittanut saksalainen SMS-Demag (nykyään SMS-Siemag) ja se toimii koko valssauslinjan prosessinohjausjärjestelmänä. Järjestelmä suorittaa jokaiselle valssattavalle aihiolle pistosarjanlaskennan etuvalssaimelle, steckel-valssaimelle ja tandem-valssaimille. Laskentamalliin tarvittavat aihion perustiedot järjestelmä saa tuotannonohjausjärjestelmä QMatolta. Pistosarjalaskennan lisäksi SMSD hoitaa muun muassa nauhakelaimen asettelut ja kuumanauhan profiili- ja tasomaisuusohjaukset. Järjestelmän palvelinympäristönä toimii vuonna 2004 hankittu klusteroitu HP-UX-palvelinympäristö.

Valssihiomossa käytössä on kaksi järjestelmää, VASE ja Pomini. VASE:lla, eli valssien seurantaohjelmalla hallitaan valssien hiontaa sekä seurataan muun muassa laakeriperiä ja hiomakiviä. Valssienvaihdosta VASE lähettää tiedot SMSD-järjestelmälle, joka puolestaan lähettää VASE:lle valsseilla ajetut tuotantolukemat. VASE-järjestelmä on käyttöönotettu vuonna 1987, eli samana vuonna, kun Tornion kuumavalssaamo on aloittanut toimintansa. Järjestelmän alkuperäinen palvelinympäristö oli OpenVMS, mutta se on siirretty Windows-ympäristöön vuonna 2005. Sovelluspalvelin on virtualisoitu vuonna 2012 ja nykyinen käyttöjärjestelmä on Windows 2003 Server.

VASE kerää hiontatietoja Pomini-järjestelmältä, millä ohjataan valssihiontakoneita. Pomini-järjestelmän työasemilla ohjataan valssihiomakoneita ja niiden kautta hionta- ja prosessitiedot tallennetaan järjestelmän tietokantaan. Pomini-järjestelmä on käyttöönotettu vuonna 2002 ja tietokantapalvelin on virtualisoitu vuonna 2012. Tietokantapalvelimen käyttöjärjestelmänä on Windows 2003 Server.

COS eli kupu-uunien prosessinohjausjärjestelmä on käyttöönotettu vuonna 2007 KUPU-projektissa. Käsiteltävien rullien työjonon suunnittelu tehdään QMatossa ja QMato lähettää rullien tiedot COS:lle. COS-järjestelmä päättelee rullien tietojen perusteella oikean hehkutusohjelman ja välittää tiedot automaatiojärjestelmälle. Automaatiojärjestelmä lähettää tietoa prosessin eri vaiheista COS:lle, joka lähettää tiedot myös QMatolle. COS-järjestelmän palvelinympäristönä toimii fyysinen Windows XP-työasema. Palvelinympäristöä ei ole mahdollista virtualisoida, koska työasemaan on

integroitu erikoiskortteja prosessinohjausjärjestelmän ja automaatiojärjestelmän kommunikointia varten.

HotSIS toimii valssauslinjan pinnantarkistusjärjestelmänä. Järjestelmään on integroitu konenäkökameroita, jotka kuvaavat valssatun kuumanauhan pintaa ylä- ja alapuolelta. Järjestelmä tutkii kameroilla otetut kuvat ja opetusmateriaalin perusteella järjestelmä etsii kuvista toistuvia ja yksittäisiä pintavirheitä. HotSIS saa valssattavan aihion perustiedot SMSD-järjestelmältä ja lähettää tarkistetun kuumanauhan tiedot kylmävalssaamon PIHA-järjestelmälle. HotSIS-järjestelmä on käyttöönotettu vuonna sovellus- ja tietokantapalvelinympäristöinä ovat fyysiset Windows 2003 Server-käyttöjärjestelmän palvelimet.

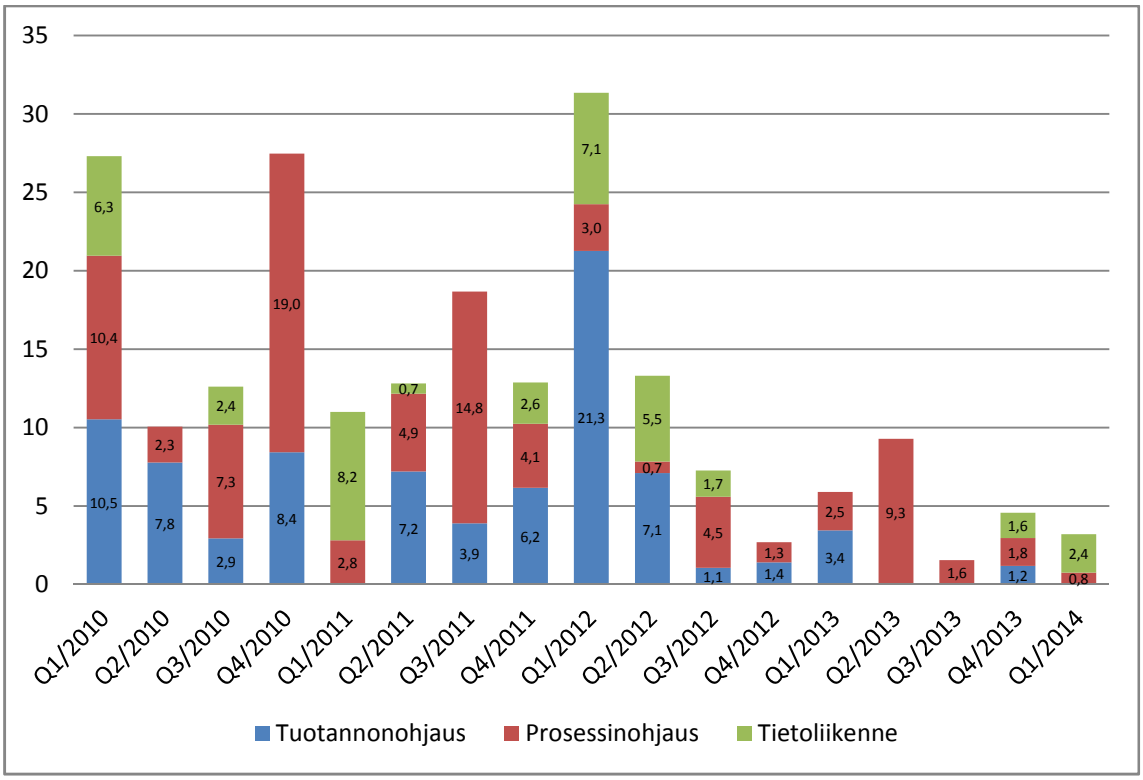
Voice Guidance on järjestelmä, joka ilmoittaa valssauslinjan tapahtumista valvomoihin. Järjestelmä on käyttöönotettu vuonna 1999, jolloin palvelinympäristönä oli fyysinen palvelin Windows 2000-käyttöjärjestelmällä. Järjestelmän palvelinympäristö on virtualisoitu vuonna 2012 ja nykyään käyttöjärjestelmänä on Windows 2008 Server. Järjestelmä saa herätteitä valssauslinjan automaatiojärjestelmiltä (Siemens ja Hitachi) ja lähettää määritellyistä tapahtumista viestin valvomoiden työasemissa olevaan client-sovellukseen. Client-sovellus päättelee viestin perusteella oikean soitettavan äänitiedoston ja näin jokaisessa valvomossa kuuluu esimerkiksi ääni ”Aihion panostus valmis”, kun aihio on panostettu askelpalkkiuuniin.

PMS eli Plant Monitoring System on saksalaisen SMS-Demagin (nykyään SMS-Siemang) toimittama kunnonvalvontajärjestelmä, joka tallentaa valssauslinjalta mittaussignaaleja, esimerkiksi valssausvoima ja jäähdytysveden virtaustietoja. Järjestelmä on käyttöönotettu vuonna 2009 ja mittausdatan analysointiin on käytössä monia työkaluja ja web-käyttöliittymä.

4.1.3 Kuumavalssaamon IT-häiriöt

Kuvassa 6 on tuntimäärinä kuumavalssaamolla kirjatut pysäyttävät häiriöt 1.1.2010 – 31.3.2014 väliseltä ajalta kvartaaleittain, jotka ovat aiheutuneet IT-järjestelmistä. Sinisellä värillä on tuotannonohjausjärjestelmästä (L3) aiheutuneet häiriöt, punaisella prosessinohjausjärjestelmistä (L2) ja vihreällä värillä tietoliikenneviat, jotka

todellisuudessa ovat joko L3- tai L2-vikoja tai muita IT-vikoja (verkkoliikenne, työasema ja niin edelleen). Tiedot on haettu QMaton häiriönhallinnasta, johon kuumavalssaamon henkilökunta kirjaa pysäyttävät häiriöt.



Kuva 6. Kuumavalssaamon pysäyttävät IT-häiriöt

Kuvan 6 perusteella viime vuosina pisimmät tuotannonohjausjärjestelmästä aiheutuneet häiriöt ovat ajalta Q1/2012. Tällöin QMatossa oli lukuisia ongelmatilanteita, joiden juurisyynä oli järjestelmän kommunikaatiopalvelun suuri epävakaus. Järjestelmään tehtiin laaja arkkitehtuurillinen muutos, jossa kommunikaatiopalvelu vaihdettiin toiseen tuotteeseen toukokuussa 2012. Tämän jälkeen pysäyttävien häiriöiden määrä on pudonnut merkittävästi tuotannossa.

Prosessinohjausjärjestelmistä aiheutuneet pysäyttävät häiriöt ovat olleet viimeisen kaksi vuotta myös vähäisiä. Alpha-järjestelmän ohjelmistopalvelimen vikaantuminen lokakuussa 2010 aiheutti merkittävimmät pysäyttävät häiriöt prosessinohjausjärjestelmistä johtuen.

5 KUUMAVALSSAAMON IT-JÄRJESTELMIEN RISKIANALYYSI

Kuumavalssaamon IT-järjestelmien riskianalyysistä oli tarkoitus tehdä mahdollisimman käyttökelpoinen ja helposti sovellettava myös muiden tuotantolinjojen IT-järjestelmien riskianalyysiä varten. Riskianalyysissä ei ole lueteltu yksittäisiä uhkia ja arvioitu niiden vaikutuksia ja todennäköisyyksiä, vaan tarkoituksena on ollut luoda mahdollisimman laaja eri osa-alueista muodostuva kokonaiskuva tehdasjärjestelmien nykytilanteesta.

5.1 Riskianalyysin osa-alueet

Järjestelmien riskianalyysi käsittelee kolmea eri osa-aluetta; palvelin-, työasema- ja sovellusympäristöä. Näiden osa-alueiden sisällä on joukko erilaisia riskitekijöitä, joille on määritelty riskiluku taulukon 1 mukaisesti. Seuraavissa kappaleissa on esitelty jokaisen osa-alueen arviointia.

5.1.1 Palvelinympäristön riskit

Palvelinympäristön riskit on jaettu seuraaviin alueisiin:

- palvelimien ikä
- varalaitteisto ja varmennus
- tuki ja huoltosopimus.

Palvelimien iän aiheuttama riskiluku on määritelty siten, että alle neljä vuotta vanha sovellus- tai tietokantapalvelin saa riskiluvuksi 0 (ei riskiä), alle seitsemän vuotta vanhan riskiluku on 1 (matala riski), alle kymmenen vuotta vanhan 2 (keskimääräinen riski) ja yli kymmenen vuotta vanhojen riskiluku tässä osiossa on 3 (korkea riski).

Varalaitteisto ja varmennuksen riskiluku määräytyy varmennustavasta. Mikäli palvelimet ovat virtualisoituja, riskiluku on tässä tapauksessa 0 (ei riskiä). Jos palvelimet ovat fyysisiä, mutta varmennus on tehty klusteroinnilla, riskiluku on 1 (matala riski). Jos fyysisen palvelimen varmennus on tehty kahdennuksella, riskiluku on

2 (keskimääräinen riski). Varalaitteen tai varmennuksen puuttuessa riskiluku on 3 (korkea riski).

Taulukossa 4 on esitelty järjestelmien palvelinympäristön riskiluvut. Kolmessa tapauksessa riskilukujen summa on nolla. Syynä tähän on se, että kyseisten järjestelmien palvelinympäristöt ovat virtualisoitu kahden viimeisen vuoden aikana ja ovat nykyisen palvelimien palveluntarjoajan tuen piirissä.

Alpha- ja APU2-optimointi-järjestelmien riskiluvut ovat samat, koska järjestelmillä on sama palvelinympäristö. Näiden järjestelmien merkittävin riski on vuonna 1997 hankittu palvelinympäristö. Palvelimille on kuitenkin olemassa huoltosopimus ulkopuolisen palveluntarjoajan kanssa, joka hieman pienentää järjestelmien palvelinympäristön riskiä. Koska kyseessä on vanha palvelinympäristö, myös suurin osa varaosista on kertaalleen käytettyjä ja kunnostettuja.

Taulukko 4. Järjestelmien palvelinympäristön riskiluvut

	Palvelinympäristö				
Järjestelmä	**Sovellus-palvelimen ikä**	**Tietokanta-palvelimen ikä**	**Varmistus**	**Palvelimen tuki/ huoltosopimus**	**Palvelinympäristön riskiluku (0-12)**
QMato	1	0	1	0	2
Alpha	3	3	2	0	8
APU1 optimointi	1	1	2	3	7
APU2 optimointi	3	3	2	0	8
SMSD	2	2	1	0	5
VASE	0	0	0	0	0
Pomini	0	0	0	0	0
COS	0	0	2	0	2
HotSIS	2	2	3	0	7
Voice Guidance	0	0	0	0	0
PMS	1	1	3	3	8

5.1.2 Työasemaympäristön riskit

Järjestelmien työasemaympäristön riskit on jaettu seuraaviin alueisiin:

- työasemien keskimääräinen ikä
- tuki
- resurssit.

Työasemien iän aiheuttama riskiluku on määritelty lähes samalla periaatteella palvelinympäristön iän arviointi. Alle kolme vuotta vanha työasema saa riskiluvuksi 0 (ei riskiä), alle kuusi vuotta vanhan riskiluku on 1 (matala riski), alle kahdeksan vuotta vanhan 2 (keskimääräinen riski) ja yli kahdeksan vuotta vanhojen riskiluku tässä osiossa on 3 (korkea riski).

Työasematuen arvioinnissa on kolme eri kategoriaa: kyllä, osittain ja ei. Mikäli järjestelmien työasematuki on täysin IT-organisaatiolla, riskiluku on 0 (ei riskiä). Mikäli tuki on vain osittaista, riksiluvuksi määräytyy 2 (kohtalainen riski). Mikäli tukea ei ole lainkaan, riskiluku on 3 (korkea riski). Tuen ollessa osittaista tai mikäli IT-organisaatio ei tarjoa tukea lainkaan, ylläpitovastuu on tässä tapauksessa pääosin tuotanto-organisaatiolla.

Resurssien riskiluvun arviointi on siten, että asiantuntijat on jaettu kahteen eri rooliin: Päätoiminen asiantuntija ja sivutoiminen asiantuntija. Päätoiminen asiantuntija tuntee järjestelmien työasemaympäristön ja vastaa uusien työasemien hankinnoista ja asennuksista kyseiselle alueelle. Sivutoiminen asiantuntija toimii jonkin toisen alueen, esimerkiksi kylmävalssaamon tuotannon työasemien päätoimisena asiantuntijana, mutta pystyy tarvittaessa tekemään tukitöitä myös toiselle alueelle. Koska asiantuntijat on jaettu kahteen eri rooliin, niillä on myös omat painoarvonsa. Päätoiminen asiantuntijan kerroin on 1,0 ja sivutoimisen 0,5. Toisin sanoen, kaksi sivutoimista asiantuntijaa vastaa yhtä päätoimista asiantuntijaa. Resurssien riskiluku on määritelty siten, että asiantuntijaluvun ollessa vähintään 2,0, riskiluku on 0 (ei riskiä). Mikäli asiantuntijaluku on 1,5, riskiluvuksi määräytyy 1, (matala riski). Mikäli asiantuntijaluku on 1,0, riskiluvuksi saadaan 2 (kohtalainen riski). Asiantuntijaluvun ollessa arvoa 1,0 vähemmän, riskiluku on 3 (korkea riski).

Taulukossa 5 on esitelty järjestelmien työasemaympäristön riskiluvut. Työasemien keskimääräinen ikä on riskeistä kaikkein pienen, koska tällä hetkellä työasemia uusitaan kolmen – neljän vuoden välein. Suurimmat riskit ovat tuessa ja resursseissa. Lähes kaikki kuumavalssaamon prosessinohjausjärjestelmien työasematuki on pääosin tuotanto-organisaatiolla ja sielläkin yhden asiantuntijaresurssin varassa. Esimerkiksi terässulatolla ollaan prosessinohjausjärjestelmien osalta samassa tilanteessa kuin mitä QMato-järjestelmän osalta, eli tilanne on paljon parempi. PMS-järjestelmän työasemaympäristön riskiluku on nolla, koska tätä järjestelmää ei käytetä tuotannon työasemissa. Järjestelmän työasemaympäristö on pääasiassa toimistotyöasemat, koska kyseessä on prosessilinjan kunnonvalvonta- ja monitorointijärjestelmä.

Taulukko 5. Järjestelmien työasemaympäristön riskiluvut

	Työasemaympäristö			
Järjestelmä	**Tuotannon työasemien keskimääräinen ikä**	**Työasematuki IT-organisaatiolla**	**Resurssit**	**Työasemaympäristön riskiluku (0-9)**
QMato	0	0	1	1
Alpha	0	2	2	4
APU1 optimointi	0	3	3	6
APU2 optimointi	0	3	3	6
SMSD	0	2	2	4
VASE	0	2	2	4
Pomini	0	3	3	6
COS	0	3	3	6
HotSIS	2	2	3	7
Voice Guidance	0	2	2	4
PMS	0	0	0	0

5.1.3 Sovellusalueen riskit

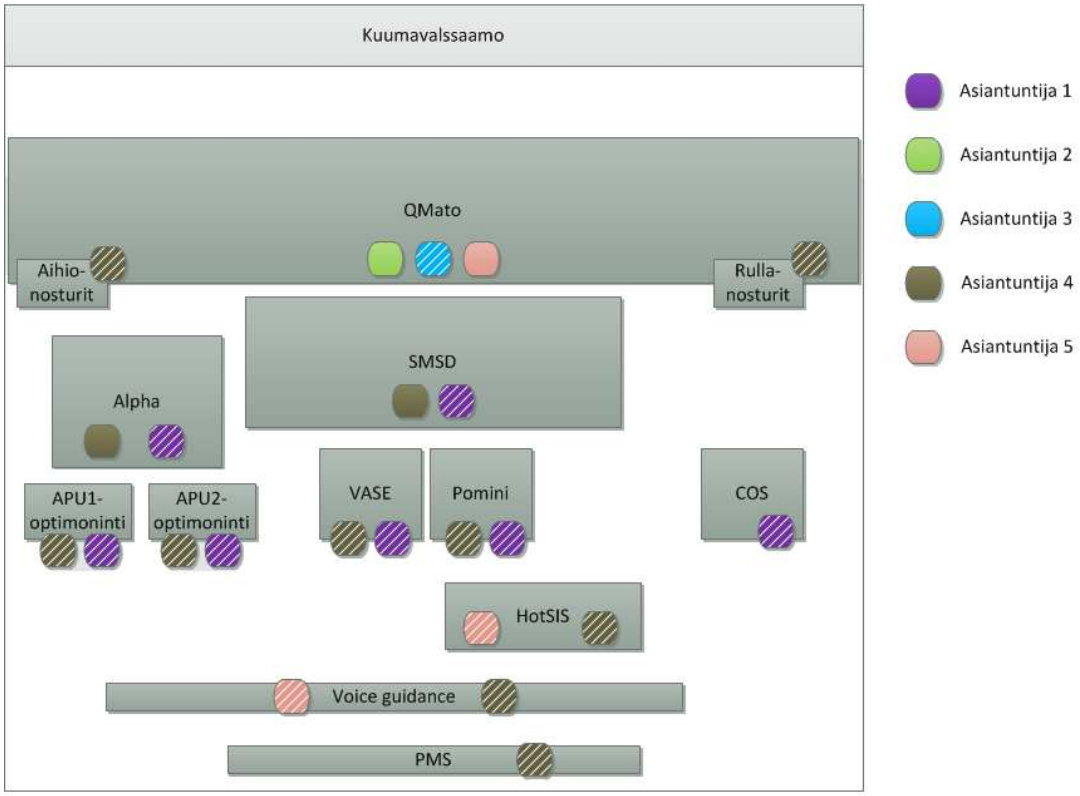
Järjestelmien sovellusympäristön riskit on jaettu seuraaviin alueisiin:

- lähdekoodien omistus
- muutostenhallinta
- resurssit.

Lähdekoodien omistuksesta tuleva riskiluku on joko 0 (ei riskiä) tai 3 (korkea riski). Muutostenhallinnassa eli vuotuisten päivitysten ja muutostöiden osalta riskiluku on määritelty siten, että mikäli järjestelmään ei tehdä muutostöitä, riskiluku on 0 (ei riskiä). Mikäli sovelluksiin tehdään alle neljä vuotuista päivitystä, on riskiluku tässä tapauksessa 1 (matala riski). Jos vuotuisia päivityksiä viidestä seitsemään, riskiluku on 2 (keskimääräinen riski). Tätä suuremmat määrät saavat riskiluvuksi 3 (korkea riski).

Resurssien riskiluvun laskemisessa on täysin sama periaate kuin mitä työasemaympäristössä. Sovelluksen päätoiminen asiantuntija vastaa järjestelmän kehitystyöstä ja pystyy korjaamaan yli 90 prosenttia järjestelmävirheistä. Sivutoiminen asiantuntija toimii asiantuntijatehtävissä jollekin toiselle järjestelmälle, mutta vastaa järjestelmän ylläpidosta esimerkiksi silloin, kun järjestelmän päätoiminen asiantuntija on lomalla.

Kuvassa 7 on havainnollistettu kuumavalssaamon tehdasjärjestelmien asiantuntijaresurssit. Kuvassa yksivärinen asiantuntijaikoni kuvaa järjestelmän päätoimista asiantuntijaa ja raidallinen ikoni järjestelmän sivutoimista asiantuntijaa. Kuten kuvasta ilmenee, tehdasjärjestelmien ja varsinkin prosessinohjausjärjestelmien asiantuntijuus on todella vähäisten resurssien varassa. Käytännössä kaksi asiantuntijaa vastaa koko tuotantolinjan prosessinohjausjärjestelmistä.



Kuva 7. Kuumavalssaamon tehdasjärjestelmien asiantuntijaresurssit

Taulukosta 6 ilmenee sovellusympäristön riskiluvut. Kuumavalssaamon IT-järjestelmistä vain osasta lähdekoodit eivät ole Outokummun omistuksessa. Vuosittaisten päivitysten määrä on pyritty pitämään maksimissaan neljässä, mutta etenkin QMato on varsin muutosaltis järjestelmä. Toki yksi syy tähän on se, että kyseessä on laaja tuotannonohjausjärjestelmä.

Taulukko 6. Järjestelmien sovellusympäristön riskiluvut

	Sovellusympäristö			
Järjestelmä	Lähdekoodit	Vuosittaisten päivitysten lukumäärä	Resurssit	Sovellusympäristön riskiluku (0-9)
QMato	0	2	0	2
Alpha	0	0	1	1
APU1 optimointi	0	0	2	2
APU2 optimointi	0	0	2	2
SMSD	0	1	1	2
VASE	0	1	2	3
Pomini	3	0	2	5
COS	0	0	1	1
HotSIS	3	0	2	5
Voice Guidance	0	0	2	2
PMS	3	0	3	6

5.2 Riskianalyysin tulokset

Taulukossa 7 on koottu kaikkien kolmen eri osa-alueen riskiluvut yhteen. Tämän lisäksi järjestelmille on annettu oma tuotantokriittisyyskerroin väliltä yhdestä neljään. Mitä suurempi järjestelmän tuotantokriittisyys on, sitä suurempi on tämä luku. Luokittelu on tehty seuraavasti:

- järjestelmän toimimattomuus pysäyttää tuotantolinjan välittömästi (4)
- järjestelmän toimimattomuus hidastaa merkittävästi tuotantolinjaa ja pysäyttää sen viimeistään kahden tunnin päästä (3)
- hidastaa tuotantoa, mutta tuotantoa pystytään jatkamaan yksi työvuoro (kahdeksan tuntia) ilman järjestelmää (2)
- ei vaikutusta tuotantoon (1).

Taulukon sarake ”järjestelmän riskiluku” on järjestelmän palvelin-, työasema- ja sovellusympäristöjen riskilukujen summa. Taulukon viimeinen sarake eli ”riskiluku suhteessa kriittisyyteen” on edellisen sarakkeen ja järjestelmän tuotantokriittisyysasteen tulo. Esimerkiksi VASE-järjestelmälle luku on 21 (3x7).

Kaiken kaikkiaan kuumavalssaamon järjestelmien kokonaisriskiluvut ovat vielä siedettävällä tasolla. Sovellusympäristön näkykulmasta asiat ovat hyvällä tasolla, mutta varsinkin työasemaympäristössä yli puolet järjestelmistä vaatii välittömiä toimenpiteitä. Palvelinympäristön osalta tilanne on hyvin pitkälti sama kuin mitä työasemaympäristössä. Merkittävin syy järjestelmien riskiluvun suuruuteen on järjestelmien vanheneva laitekanta.

Taulukko 7. Järjestelmien riskianalyysin tulokset

Järjestelmä	Järjestelmän tuotantokriittisyys (1-4)	Palvelin-ympäristön riskiluku (0-12)	Työasema-ympäristön riskiluku (0-9)	Sovellus-ympäristön riskiluku (0-9)	Järjestelmän riskiluku (0-30)	Riskiluku suhteessa kriittisyyteen
QMato	4	2	1	2	5	20
Alpha	4	8	4	1	13	52
APU1 optimointi	2	7	6	2	15	30
APU2 optimointi	2	8	6	2	16	32
SMSD	4	5	4	2	11	44
VASE	3	0	4	3	7	21
Pomini	3	0	6	5	11	33
COS	3	2	6	1	9	27
HotSIS	2	7	7	5	19	38
Voice Guidance	2	0	4	2	6	12
PMS	1	8	0	6	14	14

6 KEHITYSSUUNNITELMA

Tässä kappaleessa on kuvattu Tornion kuumavalssaamon IT-palveluiden kehityssuunnitelma seuraavaksi neljälle vuodelle. Kehityssuunnitelma perustuu pitkälti järjestelmien riskianalyysin tuloksiin ja kehityssuunnitelman tavoitteena on parantaa järjestelmien toimintaympäristöjä.

6.1 Vuosi 2014

6.1.1 Windows 7-käyttöjärjestelmän käyttöönotto tuotannon työasemissa

Windows XP-käyttöjärjestelmä on käytössä lähes kaikissa kuumavalssaamo tuotannon työasemissa. Koska käyttöjärjestelmän tuki loppuu keväällä 2014, täytyy työasemat päivittää uudempaan Windows 7-käyttöjärjestelmään. Päivityksen myötä valvomoihin tulee uudet työasemat ja lisäksi työasemien tuki saadaan siirrettyä IT-organisaatiolle.

Taulukossa 8 on havainnollistettu järjestelmien työasemaympäristön riskiluvun muuttuminen kyseisen päivityksen myötä. Alun perin lähes kaikki tuotannon työasemat ovat suhteellisen uusia, ainoa parannus tapahtuu HotSIS-järjestelmään, koska päivityksen myötä nauhakelaimen valvomosta saadaan yksi vanha Windows 2000-käyttöjärstelmällä toimiva työasema päivitettyä huomattavasti uudempaan. Merkittävimmät riskiluvun parannukset tapahtuvat työasemantuen siirtymisessä IT-organisaatiolle. Tämä vaikuttaa myös resurssien riskiluvun paranemiseen. Toki resurssien osalta riskiluvun pienentyminen vaatii perehdytystä ja koulutusta.

Kokonaisuudessaan tällä toimenpiteellä saadaan päivitettyä 16 tuotannon työasemaa kuumavalssaamolta. Tavoitteena on rakentaa yksi työasema, mihin tullaan asentamaan kaikki tarvittavat tehdasjärjestelmät. Käyttäjätilistä riippuen on tehtävä rajaukset, mitä tehdasjärjestelmiä ja millä käyttöoikeuksilla niitä voi käyttää. Kun työasema on testattu ja todettu toimivaksi, työaseman kokoonpano kloonataan jokaiseen uuteen työasemaan. Liitteessä 3 on esitelty tarkempi tehdasjärjestelmien asennussuunnitelma työasemaan.

Käytännössä tässä päivityksessä tullaan luomaan yksi tuotannon työasema, minkä voi ottaa käyttöön millä tahansa kuumavalssaamon prosessipaikalla, lukuun ottamatta

valssihiomoa ja kupu-uuneja. Syynä tähän on se, että valssihiomon Pomini-järjestelmään ja kupu-uunien COS-järjestelmään integroidut työasemat sisältävät profibus-erikoiskortteja, joilla hoidetaan kommunikointi valssihiomakoneiden automaatiojärjestelmien kanssa. Molempien järjestelmien työasemat tulevat vaatimaan omat selvityksensä.

Taulukko 8. Järjestelmien työasemaympäristön riskiluvun muutos Windows 7 käyttöönoton jälkeen

Työasemaympäristö				
Järjestelmä	Tuotannon työasemien ka. ikä	Työasematuki IT-organisaatiolla	Resurssit	Työasema-ympäristön riskiluku (0-9)
QMato	0	0	1	1
Alpha	0	0	1	1
APU1 optimointi	0	0	1	1
APU2 optimointi	0	0	1	1
SMSD	0	0	1	1
VASE	0	0	1	1
Pomini	0	3	3	6
COS	0	3	3	6
HotSIS	1	2	3	6
Voice Guidance	0	0	1	1
PMS	0	0	0	0

6.1.2 Alpha-järjestelmän palvelinympäristön päivitys

Kuten taulukosta 4 voidaan havaita, Alpha-järjestelmän palvelinympäristön riskiluku on tuotantokriittisimmistä tehdasjärjestelmistä kaikkein suurin. Syynä tähän on alkuperäinen vuonna 1997 hankittu palvelinympäristö, joka olisi pitänyt uusia jo viime vuosikymmenen puolella. Palvelinympäristölle on olemassa huoltosopimus ulkopuolisen palveluntarjoajan kanssa, joka on todettu hyväksi ja toimivaksi, mutta tuotannon määrän kasvaessa hidastaviin ja pysäyttäviin järjestelmävirheisiin ei ole varaa.

Alpha-järjestelmän palvelinympäristö on korvattavissa virtualisoituun Linux-ympäristöön, koska nykyiselle käyttöjärjestelmälle käännetyt ohjelmistot ovat lähes yhteensopivia Linux-käyttöjärjestelmän kanssa. Koska kyseessä on tuotantokriittinen järjestelmä, ohjelmistojen kattava ja systemaattinen testaus nousee avainasemaan. Järjestelmässä on lukuisia liitäntöjä automaatio- ja muihin prosessin- ja tuotannonohjausjärjestelmiin, joka tulee vaatimaan pitkäjaksoista testaamista ja simulointia. Paras tapa toteuttaa testaus olisi kaiuttaa tuotantoympäristössä liikkuvat sanomat kehitysympäristöön, jolla voitaisiin simuloida mahdollisimman todellisia tilanteita.

Moderni palvelinympäristö toki vähentää ikääntyvän laitteiston riskiä, mutta parantaa merkittävästi myös järjestelmän varmistusta ja varmuuskopioiden ottoa. Taulukosta 9 ilmenee järjestelmän palvelinympäristön riskiluvun muutos virtualisoinnin jälkeen.

Taulukko 9. Alpha-järjestelmän palvelinympäristön riskiluvun muutos virtualisoinnin jälkeen

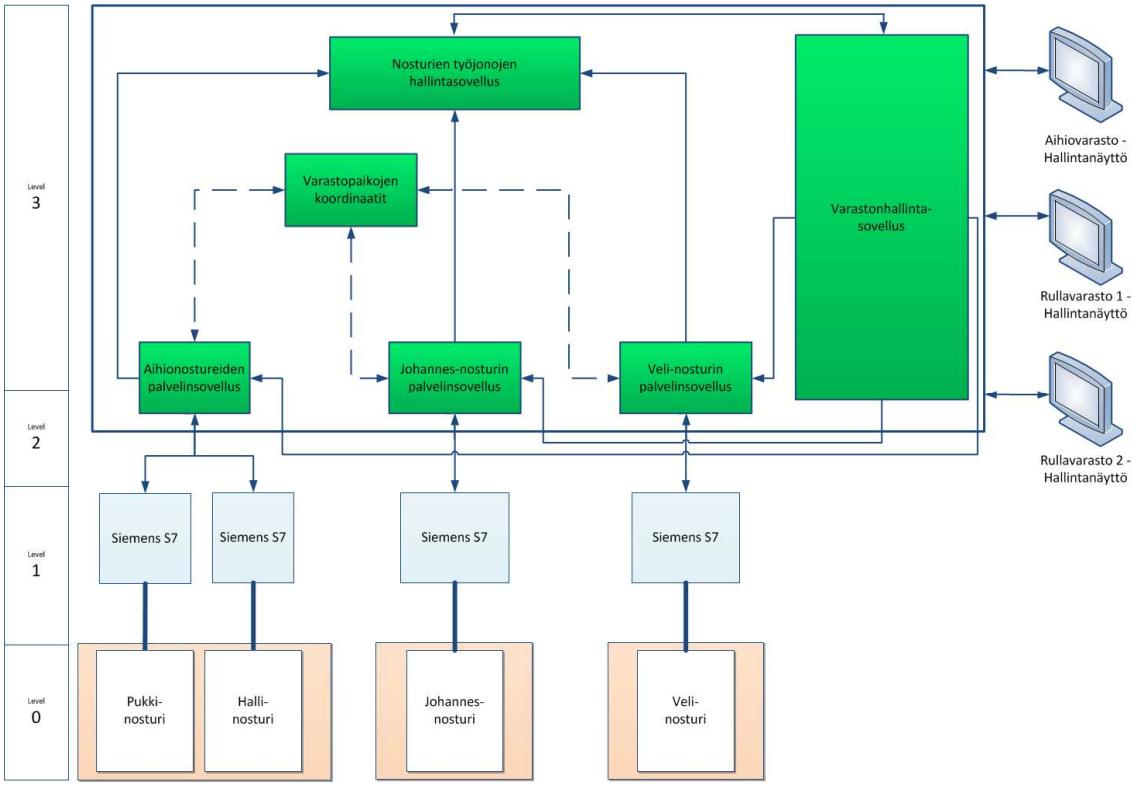
Palvelinympäristö					
Järjestelmä	Sovellus-palvelimen ikä	Tietokanta-palvelimen ikä	Varmistus	Palvelimen tuki/ huoltosopimus	Palvelinympäristön riskiluku (0-12)
Alpha	↑ 0	↑ 0	↑ 0	— 0	↑ 0

6.1.3 Automaattinostureiden simulointiympäristö

Kuumavalssaamolla on neljä Konecranesin toimittamaa automaattinosturia, joiden ohjaus ja työjonojen hallinta tapahtuu QMato-järjestelmässä. Kuumavalssaamon aihiovarastossa on kaksi nosturia, Halli ja Pukki sekä molemmissa rullavarastoissa omat nosturinsa Johannes ja Veli. Halli- ja Pukki-nosturien ohjaukseen QMatossa on yksi yhteinen palvelinsovellus ja rullavarastojen nostureille omat sovelluksensa. Kuvassa 6 on esitelty kuumavalssaamon automaattinosturien hallinta QMato-järjestelmässä.

Kuten kuvasta 8 näkee, nostureiden ja QMaton välinen kommunikointi on QMato-järjestelmästä katsottuna lähes samanlainen. Automaattinostureiden simulointiympäristöön tarvittaisiin yksi Siemensin S7-sarjan logiikkaohjain, mihin

pitäisi ohjelmoida QMaton ja nostureiden kommunikointitoiminnot. Koska nostureiden toimittaja on sama, myös ohjaussanomien rakenne on täysin sama jokaisen nosturin integraatiossa. Tämän vuoksi yhdellä logiikkaohjaimella pystyttäisiin simuloimaan aina yhden nosturin toimintoja kerrallaan ja nosturiympäristön vaihtaminen toiseen tapahtuisi QMatosta. Simulointiympäristö parantaisi huomattavasti QMatoon liittyvien nosturitoimintojen muutostöiden ja virheenkorjausten testaamista ja näin käyttöönotoissa ei tulisi yllättäviä ongelmatilanteita vastaan.



Kuva 8. Kuumavalssaamon automaattinosturien hallinta QMato-järjestelmässä

6.2 Vuosi 2015

6.2.1 HotSIS-järjestelmän virtualisointi

HotSIS-järjestelmässä on kaksi fyysistä palvelinta, joista toisessa on järjestelmän tietokanta. Tämän lisäksi kokoonpanoon kuuluu seitsemän työasemaa, joilla hoidetaan järjestelmän konfiguraatiota ja konenäköjärjestelmän tuottaman mittausdatan laskentaa. Kyseiset työasemat poikkeavat valvomotyöasemista hieman, sillä niiden käyttöaste on

huomattavasti vähäisempää ja käyttäjinä ovat pinnanlaadun kehityksestä ja tutkimuksesta vastaavat henkilöt.

Osa työasemista on jo päivitetty Windows 7 -käyttöjärjestelmään, mutta suurimmalla osalla käyttöjärjestelmä on Windows XP. Koska työasemien operointi on vähäistä, olisi tehokkainta virtualisoida sekä järjestelmän palvelinympäristö että työasemaympäristö, pois lukien valvomoissa olevat työasemat. Tällä hetkellä nykyinen palveluntarjoaja tarjoaa sekä palvelimille että työasemille virtualiympäristön. Virtualisoidut palvelin- ja työasemaympäristöt vähentäisivät merkittävästi HotSIS-järjestelmän riskialttiutta, etenkin vanhenevan laitekannan suhteen. Taulukossa 10 on esitetty järjestelmän palvelin- ja työasemaympäristöjen riskiluvun muuttuminen virtualisoinnin jälkeen.

Taulukko 10. HotSIS-järjestelmän riskiluvun muutos järjestelmän virtualisoinnin jälkeen

Palvelinympäristö					
Järjestelmä	Sovellus-palvelimen ikä	Tietokanta-palvelimen ikä	Varmistus	Palvelimen tuki/ huoltosopimus	Palvelinympäristön riskiluku (0-12)
HotSIS	⇧ 0	⇧ 0	⇧ 0	⇧ 0	⇧ 0

Työasemaympäristö				
Järjestelmä	Tuotannon työasemien ka. Ikä	Työasematuki IT-organisaatiolla	Resussit	Työasema-ympäristön riskiluku (0-9)
HotSIS	⇧ 0	⇧ 0	⇧ 1	⇧ 1

6.2.2 Valssihiomon tehdasjärjestelmien kehitysympäristö

Kokonaisuudessaan valssihiomon tehdasjärjestelmien hallinta ei ole IT-organisaatiolla niin hyvin hallinnassa kuin muissa kuumavalssaamon tehdasjärjestelmissä. Pomini- ja VASE-järjestelmät muodostavat muista kuumavalssaamon tehdasjärjestelmistä hieman erilaisemman toimintaympäristön, mikä johtuu hyvin pitkälti Pomini-järjestelmän työasemista, jotka on integroitu suoraan valssihiomakoneiden automaatiojärjestelmiin. Muissa järjestelmissä automaatiojärjestelmien integrointi on hoidettu palvelinympäristöissä.

Tämä poikkeava arkkitehtuuri edellyttää kattavaa tietämystä sekä sovellus- että työasemaympäristöjen asiantuntijoilta. Siispä tämän kokonaisuuden hallitsemisen parantamiseksi tulisi koota kattava komponenttilista työasemien erikoiskorteista ja rakentaa toimivat varalaitteet käytössä olevien työasemien vikaantumisten varalta. Sovellusympäristön näkökulmasta valssihiomon järjestelmistä pitäisi rakentaa kattava simulointiympäristö, jolla voitaisiin testata myös uudet tuotannon varatyöasemat. Tällä kehitysympäristöllä saataisiin parannettua sekä työasema- että sovellusympäristön riskialttiutta. Taulukossa 11 on esitelty valssihiomon Pomini-järjestelmän sovellus- ja työasemaympäristön riskiluvun odotettavaa muutosta kehitysympäristön käyttöönoton jälkeen.

Taulukko 11. Pomini-järjestelmän sovellus- ja työasemaympäristöjen riskiluvun odotettava muutos kehitysympäristön käyttöönoton jälkeen

Sovellusympäristö				
Järjestelmä	Lähdekoodit	Vuosittaisten päivitysten lkm	Resurssit	Sovellusympäristön riskiluku (0-9)
Pomini	— 3	— 0	↑ 1	↑ 4
Työasemaympäristö				
Järjestelmä	Tuotannon työasemien ka. Ikä	Työasematuki IT-organisaatiolla	Resussit	Työasema-ympäristön riskiluku (0-9)
Pomini	— 0	↑ 0	↑ 2	↑ 2

6.3 Vuodet 2016 ja 2017

Nykyinen valssauslinjan prosessinohjausjärjestelmän SMSD:n palvelinympäristö on vuonna 2016 jo 11 vuotta vanha. Jotta järjestelmän palvelinympäristön kanssa ei jouduttaisi samaan tilanteeseen kuin mitä askelpalkkiuunien prosessinohjausjärjestelmän Alphan kanssa on nyt, täytyy myös SMSD-järjestelmän palvelinympäristö päivittää uudempaan.

Päivityksen suurimpana ongelmana lienee nykyisen toimittajan tietotaidon ja tuen väheneminen järjestelmän nykyiselle arkkitehtuurille. Siispä pelkkä palvelinympäristön vaihtaminen esimerkiksi virtualisoituun Linux- tai Windows-ympäristöön ei välttämättä onnistu ihan helposti, koska sen myötä myös ulkopuolinen tuki vähenee entisestään. Päivitys vaatii laajemman selvityksen ja se pitäisi aloittaa jo vuoden 2016 aikana ja varsinainen työ tulisi tehdä vuoden 2017 aikana.

7 TOIMINTAMALLI – TUOTANNON TYÖASEMAN KÄYTTÖÖNOTTO

Opinnäytetyön yhtenä tavoitteena oli luoda jokin uusi toimintamalli, jolla saataisiin kehitettyä ja tehostettua IT-organisaation toimintaa. Kehityssuunnitelmassa kuvattu Windows 7-käyttöjärjestelmän asennus tuotannon työasemiin vuodelle 2014 osoittautui työksi, jonka tekeminen nykyisillä toimintamalleilla ja resursseilla ei tulisi onnistumaan kovinkaan tehokkaasti. Tämän vuoksi tuotannon työasemien käyttöönoton suunnitteluun tehtiin uusi toimintamalli.

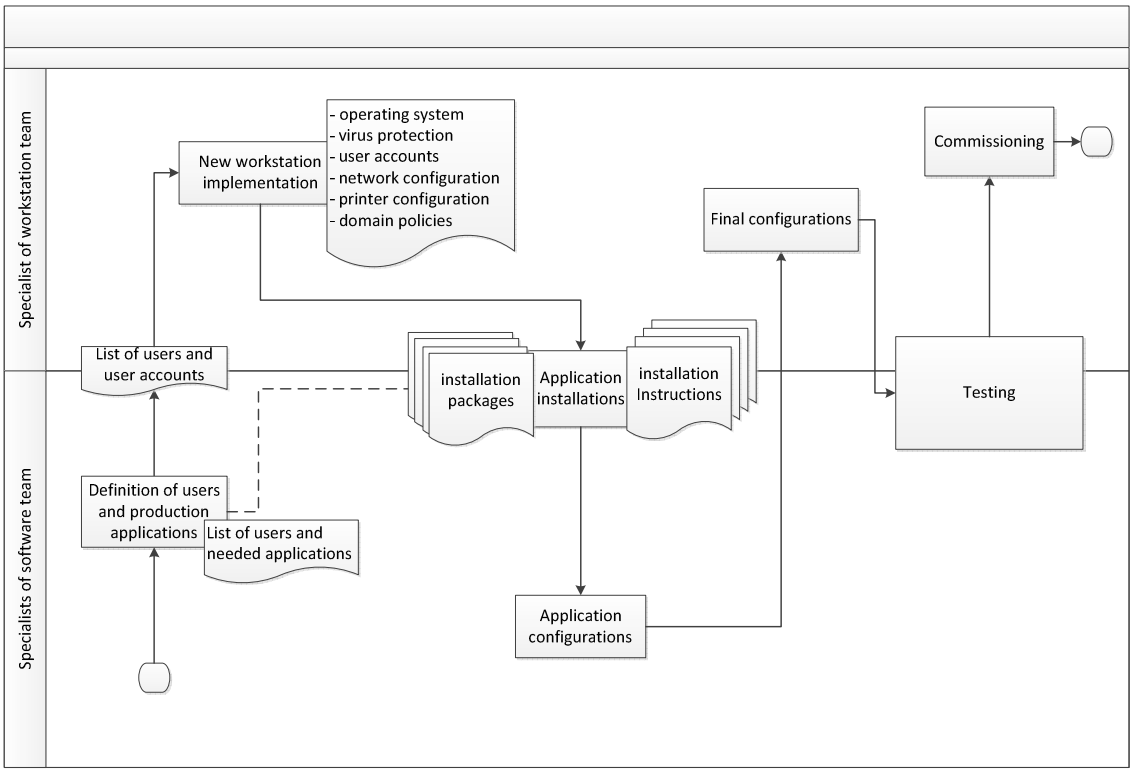
Kuvassa 9 on esitelty ensimmäinen vaihe uuden tuotannon työaseman käyttöönotosta. Tuotannon työaseman käyttöönotto alkaa sen käyttötarkoituksen antamien vaatimusten suunnittelulla. Tehdasjärjestelemistä vastaavat asiantuntijat määrittelevät tarvittavat ohjelmistot ja käyttäjät, jotka työasemaa tulevat käyttämään. Kun tämä on saatu tehtyä työasematuen asiantuntija rakentaa varsinaisen työaseman, mihin on asennettu seuraavat perusasetukset ja -ohjelmistot:

- käyttäjätilit
- tietoliikenneverkon määritykset
- tietoturvaohjelmistot (muun muassa virustorjunta ja palomuuriasetukset)
- tulostinmääritykset
- sähköposti.

Kun työaseman perusasetukset ovat valmiina, työ siirtyy tehdasjärjestelmistä vastaaville henkilöille. Yhteistyössä työasematuen kanssa, asiantuntijat asentavat tarvittavat tehdasjärjestelmien käyttöliittymäsovellukset. Työssä käytetään apuna olemassa olevia asennuspaketteja ja -ohjeita. Mikäli jonkin sovelluksen asennusohjeet ovat puutteellisia tai puuttuvat kokonaan, on asia korjattava päivittämällä ohjeita tai tekemällä ne kokonaan uusiksi. Asennusohjeet ja ohjelmistojen asennuspaketit on talletettava ennalta sovittuun paikkaan, josta ne löytyvät jatkossakin.

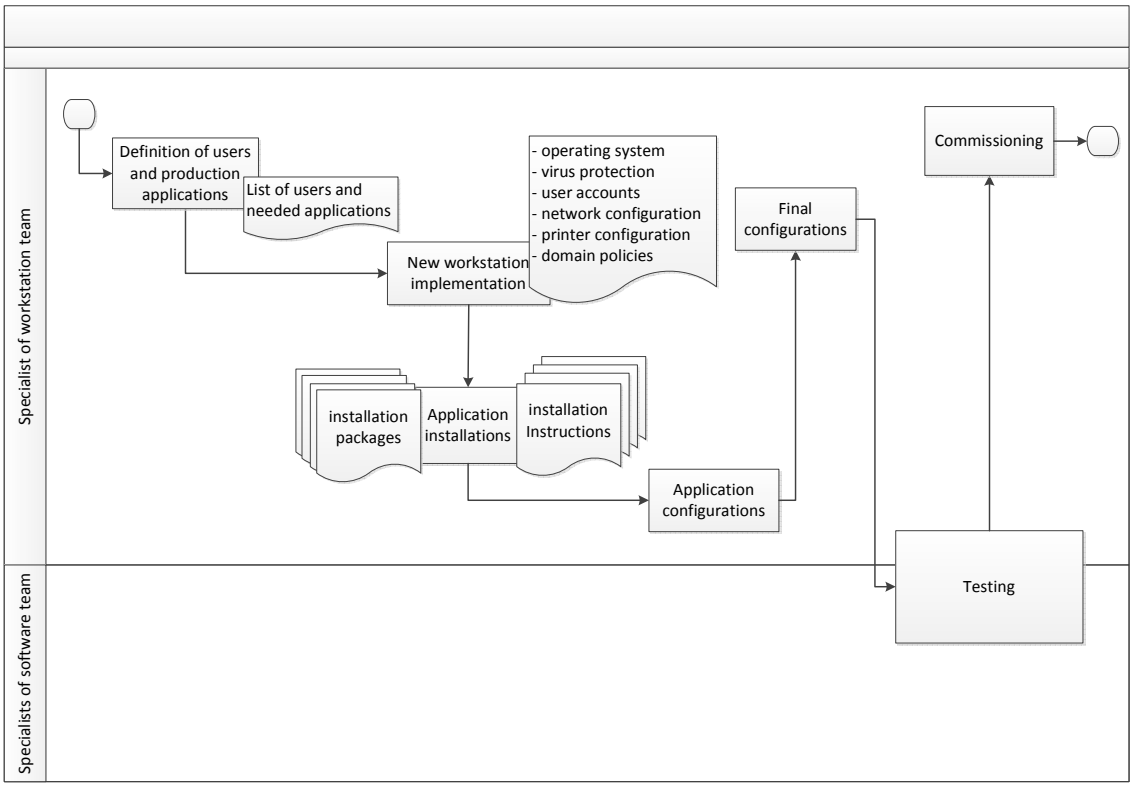
Kun työasemassa on kaikki tarvittavat ohjelmistot asennettuna, työasematuki asentaa koneeseen viimeiset tietoturvapäivitykset ja tämän jälkeen suoritetaan työaseman testaus tuotantoympäristöä vasten. Jos työasema todetaan toimivaksi, se voidaan siirtää

tuotantoon prosessipaikan valvomoon, missä työaseman testaus jatkuu varsinaisten loppukäyttäjien toimesta. Vanha työasema jätetään valvomon sähkötilaan siltä varalta, että jos uusi työasema ei toimikaan oikein. Näissä ongelmatilanteissa uusi työasema otetaan pois käytöstä ja vanha laitetaan tilalle.



Kuva 9. Toimintamallikaavio uuden tuotannon työaseman suunnittelusta

Kuvassa 10 on esitelty uuden tuotannon työaseman käyttöönotto, kun ensimmäinen vaihe on todettu valmiiksi. Tavoitteena on, että työasematuki pystyisi jatkossa yksin tuottamaan uuden työaseman lähes käyttöönottokelpoiseksi ja tehdasjärjestelmistä vastaaville asiantuntijoille jäisi osittaiseksi työksi vain ohjelmistojen lopullinen testaus ennen tuotannollista käyttöönottoa.



Kuva 10. Lopullinen toimintamallikaavio tuotannon työaseman käyttöönotosta

8 POHDINTA

Opinnäytetyön tuloksena muodostui laaja ymmärrys tietojärjestelmien riskienhallinnasta sekä kuumavalssaamon tehdasjärjestelmien nykytilasta. Tehdasjärjestelmien riskianalyysissä hyödynnettiin olemassa olevaa tietoa ja opinnäytetyön riskienhallinnan teoriaosan tuomia uusia näkökulmia.

Yleisesti ottaen tietojärjestelmien riskienhallinnan kirjallisuus pureutuu hyvin syvällisesti pelkkään tietoturvaan. Riskienhallinta on laaja käsite, mutta muusta kuin tietoturva-asioista oli vaikea löytää sopivaa lähdeaineistoa. Tietoturva-asiat ovat toki tärkeitä asioita, kun käsitellään toimintaympäristön perusinfrastruktuuria, esimerkiksi tietoliikenneverkkoa, mutta varsinkin sovellusten ja etenkin räätälöityjen tehdasjärjestelmien näkökulmasta tietoturva on hyvin pieni osa riskienhallintaa.

Kuumavalssaamon tehdasjärjestelmistä on ennenkin tehty riskianalyysejä, mutta niiden hyödyntäminen tässä opinnäytetyössä ei osoittautunut kovinkaan käyttökelpoisiksi. Nykyiset riskianalyysit ovat hyvin pitkälti listoja asioista, joille on hyvin vaikeaa luoda korjaavia toimenpiteitä. Esimerkiksi riski nimeltä ”QMato-järjestelmä ei toimi” on hyvä esimerkki nykyisestä riskianalyysin tasosta. Myös suurin osa Internetistä löydetyistä riskianalyysimalleista oli juurikin listauksia erityyppisistä riskeistä, joille oli annettu oma riskilukunsa. Riskianalyysimallia, jolla voisi verrata useamman tietojärjestelmän nykytilannetta keskenään, ei ollut tarjolla.

Opinnäytetyön tuloksena syntyi riskianalyysimalli, joka ottaa kantaa tietojärjestelmään kokonaisuutena ja antaa vertailukelpoista tietoa myös muista analysoitavista järjestelmistä. Riskianalyysin jakaminen kolmeen kategoriaan eli palvelin-, työasema- ja sovellusympäristö tuntui luonnollisesta vaihtoehdolta jakaa riskianalyysi osiin. Neljäntenä kategoriana olisi voinut olla verkkoympäristö, mutta sen lisääminen riskianalyysiin ei olisi muuttanut millään lailla järjestelmien riskilukua. Tällä hetkellä kuumavalssaamon tietoliikenneverkon hallinta on hyvällä tasolla ja sen vikasietoisuusaste on erittäin hyvä.

Työn tarkoituksena oli myös luoda kehityssuunnitelma kuumavalssaamon IT-palveluille. Kehityssuunnitelmaan tulikin asioita riskianalyysin tulosten pohjalta ja osa asioista on jo käynnistetty kevään 2014 aikana.

Kaiken kaikkiaan riskianalyysin tulokset ja kehityssuunnitelman kuvatut asiat kuvaavat hyvin laajojen, monimutkaisten ja pitkälti räätälöityjen tehdasjärjestelmien oleellisinta asiaa, eli asiantuntemusta. Räätälöityjen tehdasjärjestelmien ylläpito, kehitys ja toistuvien ongelmien juurisyiden selvitykset vaativat pitkäjänteistä paneutumista pieniinkin yksityiskohtiin, joita ei kirjoista lukemalla yksin opi. Osaaminen vaatii useamman vuoden työpanosta, joten ei ole siis pelkkää sattumaa, että järjestelmät toimivat luotettavasti.

Suurimman haasteen järjestelmien riskienhallintaan tuo kustannussäästöt. Moni asia olisi pitänyt tehdä jo vuosia sitten, mutta kustannussäästö ja rajoitettu investointibudjetti ovat olleet se ensimmäinen asia, joihin asiat ovat pysähtyneet. On pyritty etsimään korjaavia toimenpiteitä, mutta todellisuudessa niillä on saatu todellisesta riskiä vain siirrettyä. Kun tähän vielä lisätään lukumäärältään vähäiset asiantuntijaresurssit, tulee järjestelmien riskienhallinta jatkossakin olemaan entistä vaikeampaa.

9 LÄHTEET

Iivari, Mika & Laaksonen, Mika 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Helsinki: Tietosanoma Oy

Kuumavalssaamon esittelyvideo 2006. Tuotanto: SMS Demag & Bachhausen Insdustrial film/video, Düsseldorf, Saksa

Kuusela, Hannu & Ollikainen, Reijo 2005. Riskit ja riskienhallinta. Tampere. Tampereen yliopistopaino Oy

Malmén, Yngve & Wessberg, Nina. Riskienhallintaprosessi. Hakupäivä 7.5.2014 < http://www.nbcsec.fi/sptry/arkisto/art-01.pdf>

Manufacturing Operations Management. University of Cambridge. Hakupäivä 5.4.2014 <http://www.futuristix.co.za/content/S95_Tutorial.pdf>

Modeling Secure Network Architecture. Hakupäivä 18.1.2014. <http://www.robiulislam.wordpress.com/2011/12/28/modeling-secure-network-architecture>

Occupational Health and Safety Risk Assessment Sample 4x4 Risk Matrix. Hakupäivä 5.4.2014 <http://www.onsafelines.com/risk-assessment-matrix-4x4.html>

Outokumpu –kotisivut. Hakupäivä 11.12.2013 <http://www.outokumpu.com>

Outokumpu Stainless, Tornio Works, Tornion tehtaiden ja Kemin kaivoksen esittelykalvot. Hakupäivä 11.12.2013 <http://onet.outokumpu.com/en/AboutUs/Presentations/Documents/Outokumpu_Tornio%20ja%20Kemi_FI.pptx>

Pitkäranta, Ari. Työkirja laadullisen tutkimuksen tekijälle. Hakupäivä 7.5.2014 <http://www.samk.fi/download/13153_Laadullisen_tutkimuksen_tyokirja_APitkaranta.pdf>

Risk monitoring and control. Hakupäivä 7.5.2014 <http://www.cin.ufpe.br/~if717/Pmbok2000/pmbok_v2/wbs_11.6.html>

Stanford Encyclopedia of Philosophy. Hakupäivä 7.5.2014 <http://plato.stanford.edu/entries/risk/>

Suomen Automaatioseura ry 2007. Automaatiosuunnittelun prosessimalli. Helsinki

Tauriainen, Hannu 2007. Ohjelmistoalustan suunnittelu ja toteutus röntgenkuvien käsittelyyn. Opinnäytetyö. Kemi-Tornion ammattikorkeakoulu, Kemi

Windows XP:n tuki on päättymässä, Microsoft. Hakupäivä 20.1.2014 <http://windows.microsoft.com/fi-fi/windows/end-support-help>

10 LIITTEET

Liite 1. Kuumavalssaamon järjestelmien arkkitehtuurikuvaukset (luottamuksellinen)

Liite 2. Tuotannon työasemat (luottamuksellinen)

Liite 3. Tehdasjärjestelmien asennus tuotannon työasemiin (luottamuksellinen)